An Almost-Optimally Fair Three-Party Coin-Flipping Protocol

Working Draft: Please Do Not Distribute

Iftach Haitner* Eliad Tsfadia*

March 8, 2014

Abstract

In a multiparty *fair* coin-flipping protocol, the parties output a common (close to) unbiased bit, even when some corrupted parties try to bias the output. Cleve [STOC 1986] has shown that in the case of dishonest majority (i.e., at least half of the parties can be corrupted), in *any* m-round coin-flipping protocol, the corrupted parties can bias the honest parties' common output bit by $\Omega(\frac{1}{m})$. For more than two decades, the best known coin-flipping protocols against dishonest majority had bias $\Theta(\frac{t}{\sqrt{m}})$, where t is the number of corrupted parties. This was changed by a recent breakthrough result of Moran et al. [TCC 2009], who constructed an m-round, *two*-party coin-flipping protocol with optimal bias $\Theta(\frac{1}{m})$. In a subsequent work, Beimel et al. [Crypto 2010] extended this result to the multiparty case in which *less than* $\frac{2}{3}$ of the parties can be corrupted. Still for the case of $\frac{2}{3}$ (or more) corrupted parties, the best known protocol had bias $\Theta(\frac{t}{\sqrt{m}})$. In particular, this was the state of affairs for the natural three-party case.

We make a step towards eliminating the above gap, presenting an m-round, three-party coin-flipping protocol, with bias $\frac{O(\log^2 m)}{m}$. Our approach (which we also apply for the two-party case) does not follow the "threshold round" paradigm used in the work of Moran et al. and Beimel et al., but rather is a variation of the majority protocol of Cleve, used to obtain the aforementioned $\Theta(\frac{t}{\sqrt{m}})$-bias protocol.

Keywords: coin-flipping protocols; fairness; fair computation

*School of Computer Science, Tel Aviv University. E-mail: iftachh@cs.tau.ac.il,eliadtsf@post.tau.ac.il.
Research supported by ISF grant 1076/11, the Israeli Centers of Research Excellence (I-CORE) program (Center No. 4/11), US-Israel BSF grant 2010196 and Check Point Institute for Information Security.

Contents

1 Introduction

In a multiparty *fair* coin-flipping (-tossing) protocol, the parties output a common (close to) unbiased bit, even though some corrupted parties try to bias the output. More formally, such protocols should satisfy the following two properties: first, when all parties are honest (i.e., follow the prescribed protocol), they all output the *same* bit, and this bit is unbiased (i.e., uniform over $\{0,1\}$). Second, even when some parties are corrupted (i.e., collude and arbitrarily deviate from the protocol), the remaining parties should still output the *same* bit, and this bit should not be too biased (i.e., its distribution should be close to uniform over $\{0,1\}$). We emphasize that, unlike weaker variants of coin-flipping protocol known in the literature, the honest parties should output a common bit, regardless of what the corrupted parties do. In particular, they are not allowed to abort if a cheat was noticed.

When a majority of the parties are honest, efficient and *completely* fair coin-flipping protocols are known as a special case of secure multiparty computation with an honest majority [10].[1] When an honest majority is not guaranteed, however, the situation is more complex.

Negative results. Cleve [15] showed that for *any* efficient two-party m-round coin-flipping protocol, there exists an efficient adversary to bias the output of the honest party by $\Theta(1/m)$. This lower bound extends to the multiparty case via a simple reduction.

Positive results. Assuming one-way functions exist, Cleve [15] showed that a simple m-round majority protocol can be used to derive a k-party coin-flipping protocol with bias $\Theta(\frac{t}{\sqrt{m}})$ (against dishonest majority), where t is the number of corrupted parties. For more than two decades, Cleve's protocol was the best known fair coin-flipping protocol (without honest majority), under *any* hardness assumption, and for *any* number of parties. In a recent breakthrough result, Moran et al. [35] constructed an m-round, *two*-party coin-flipping protocol with optimal bias of $\Theta(\frac{1}{m})$. The result holds for any efficiently computable m, and under the assumption that oblivious transfer protocols exist. In a subsequent work, Beimel et al. [7] extended the result of [35] for the multiparty case in which *less than* $\frac{2}{3}$ of the parties can be corrupted. More specifically, for any $t < \frac{2}{3} \cdot k$, they presented an m-round, k-party protocol, with bias $\frac{2^{2t-k}}{m}$ against (up to) t corrupted parties.

Still for the case of $\frac{2}{3}$ (or more) corrupted parties, the best known protocol was the $\Theta(\frac{t}{\sqrt{m}})$-bias majority protocol of [15]. In particular, this was the state of affairs for the natural three-party case (where two parties are corrupt).

1.1 Our Result

We present an almost-optimally fair, three-party coin-flipping protocol.

Theorem 1.1 (main theorem, informal)**.** *Assuming the existence of oblivious transfer protocols, then for any $m \in$ poly there exists an m-round, three-party coin-flipping protocol, with bias $\frac{O(\log^2 m)}{m}$ (against one, or two, corrupted parties).*

As a building block towards constructing our three-party protocol, we present an alternative construction for two-party, almost-optimally fair coin-flipping protocols. Our approach does not fol-

[1] Throughout, we assume a broadcast channel is available to the parties.

lows the "threshold round" paradigm used in [35, 7], but rather is a variation of the aforementioned $\Theta(\frac{t}{\sqrt{m}})$-bias, coin-flipping protocol of [15].

1.2 Additional Related Work

Cleve and Impagliazzo [16] showed that in the *fail-stop model*, any two-party m-round coin-flipping protocol has bias $\Omega(\frac{1}{\sqrt{m}})$; adversaries in this model are computationally unbounded, but they must follow the instructions of the protocol, except for being allowed to abort prematurely. Dachman-Soled et al. [17] showed that the same holds for $o(n/\log n)$-round protocols in the random-oracle model — the parties have oracle access to a uniformly chosen function over n bit strings.

There is a vast literature concerning coin-flipping protocols with weaker security guarantees. Most notable among these are protocols that are *secure with abort*. According to this security definition, if a cheat is detected or if one of the parties aborts, the remaining parties are not required to output anything. This form of security is meaningful in many settings, and it is typically much easier to achieve; assuming one-way functions exist, secure-with-abort protocols of negligible bias are known to exist against any number of corrupted parties [12, 28, 36]. To a large extent, one-way functions are also necessary for such coin-flipping protocols [11, 27, 29, 33].

Coin-flipping protocols were also studied in a variety of other models. Among these are collective coin-flipping in the perfect information model: parties are computationally unbounded and all communication is public [4, 9, 19, 38, 39], and protocols based on physical assumptions, such as quantum computation [2, 5, 6] and tamper-evident seals [34].

Perfectly fair coin-flipping protocols (i.e., zero bias) are a special case of protocols for *fair* secure function evaluation (SFE). Intuitively, the security of such protocols guarantees that when the protocol terminates, either everyone receives the (correct) output of the functionality, or no one does. While Cleve [15]'s result yields that some functions do not have fair SFE, it was recently shown by Gordon et al. [25] that many interesting function families do have (perfectly) fair SFE.

1.3 Our Techniques

The following is a high-level description of the ideas underlying our three-party fair coin flipping protocol. We start by describing the two-party protocol of Moran et al. [35], and explain why natural extensions of their approach (such as the one used in [7]) fall short when it comes to constructing three-party fair protocols. We next explain our new approach for two-party protocols, and then extend this approach to three parties.

Throughout, we assume without loss of generality that if a corrupted party aborts in a given round, it sends an abort message to all other parties at the *end* of this round (after seeing the messages sent by the non-aborting parties). To keep the discussion simple, we focus on security against fail-stop adversaries — the parties follow the prescribed protocol, but might abort prematurely. Achieving this level of security is the heart of the matter, since (assuming one-way functions exist) there exists a round-preserving reduction from protocols secure against fail-stop adversaries into protocols of full-fledged security [22].

1.3.1 The Two-Party Protocol of Moran et al.

For $m \in \mathbb{N}$, the $(2m)$-round, two-party protocol $(\mathsf{P}_0, \mathsf{P}_1)$ of Moran et al. [35] is defined as follows.[2] Following a common paradigm for fair multiparty computations [7, 24, 31], the protocol starts by the two parties using oblivious transfer (OT) to securely compute the following "share generating" random function.

Algorithm 1.2 (share generating function $\mathsf{SharesGen}$)**.**

1. *Uniformly sample* $c \leftarrow \{0,1\}$ *and* $i^* \leftarrow [m]$ $(= \{1, \ldots, m\})$.
2. *For* $i = 1$ *to* $[m]$*, let*

   (a) $(d_i^0, d_i^1) = \begin{cases} \text{uniform } \textit{sample from } \{0,1\}^2, & i < i^* - 1 \\ (c, c), & \textit{otherwise.} \end{cases}$

   (b) $c_i = \begin{cases} \perp, & i < i^* \\ c, & \textit{otherwise.} \end{cases}$

3. *Split each of the* $3m$ *values* $d_1^0, d_1^1, \ldots, d_m^0, d_m^1, c_1, \ldots, c_m$ *into two "shares," using a 2-out-of-2 secret sharing scheme, and output the two sets of shares.*

Protocol 1.3 $((\mathsf{P}_0, \mathsf{P}_1))$**.**

Initial step: The parties securely compute the function $\mathsf{SharesGen}$*, where each party gets one set of shares.*

Main loop: For $i = 1$ *to* m*, do*

(a) P_0 *sends to* P_1 *its share of* d_i^1*, and* P_1 *sends to* P_0 *its share of* d_i^0*.*

- P_0 *reconstructs the value of* d_i^0*, and* P_1 *reconstructs the value of* d_i^1*.*

(b) *Each party sends to the other party its share of* c_i*.*

- *Both parties reconstruct the value of* c_i*.*

Output: The parties output c_i*, for the first* i *for which* $c_i \neq \perp$*.*

Abort: If P_0 *aborts, party* P_1 *outputs the value of* d_i^1 *for the* maximal $i \in [m]$ *for which it has reconstructed this value. If there is no such* i*,* P_1 *outputs a uniform bit. (The case that* P_1 *aborts is analogously defined).*

We start with few observations regarding the secure computation of $\mathsf{SharesGen}$ done in the above protocol.

- The computation of $\mathsf{SharesGen}$ is *not* fair: the parties get their parts of the output (i.e., their shares) in an *arbitrary* manner. Specifically, the corrupted party might prematurely abort after learning its part of the output, preventing the other party from getting its part.

[2] The protocol described below is a close variant of the original protocol of Moran et al. [35], which serves our presentation better.

- Since $\mathsf{SharesGen}$ is efficient (in m), assuming OT protocols exist, an (unfair) secure computation of $\mathsf{SharesGen}$ exists for any efficiently computable m.
- Ignoring negligible terms (due to the imperfection of secure computation using OT), the output of each party (when seen on its own) is a set of uniform strings. In particular, it contains *no information* about the other party's shares, or about the values of c and i^*.

  By construction, a party outputs a uniform bit if the other party aborts before the end of the secure computation phase. Hence, it makes no sense for a party to abort during this phase.
- Given the above observation, it is instructive to pretend that at the first step of the protocol, the output of a random execution of $\mathsf{SharesGen}$ was given to the parties by an *honest dealer*.

Note that in each round of the above protocol, both honest parties send their messages without waiting for the other party's message. Hence, the above protocol is symmetric with respect to the parties' role. However, since we assume no simultaneous channel (which would have trivialized the whole question), the corrupted party can postpone sending its message until it gets the message of the honest party, and then decide whether to send its message for this round or abort.

Security of the protocol. At least on the intuitive level, the security proof of the above protocol is rather simple. Since the protocol is symmetric, we assume for concreteness that P_0 is corrupted and tries to bias the expected output of P_0 away from $\frac{1}{2}$. The following random variables are defined with respect to a random execution of $(\mathsf{P}_0, \mathsf{P}_1)$: let V be the view of the corrupted P_0, right after sending the abort message, and let V^- be the value of V without this abort message (V^- and V are set to the full view, if no abort occurred). Finally, for a view v, let $\mathsf{val}(v)$ be the expected outcome of the non-aborting parties, conditioned on v, and assuming the non-aborting parties act *honestly* in the rest of the execution. It is not hard to verify that the bias obtained by P_0 is *exactly* $|\mathsf{val}(V) - \mathsf{val}(V^-)|$.

It is also easy to see that by aborting in round (i, b), for some $i \in [m]$, party P_0 gains nothing (i.e., $\mathsf{val}(V) = \mathsf{val}(V^-)$), where the (i, j)'th round of the execution stands for the j'th step of the i'th loop in the execution. A slightly more complicated math yields that by aborting in round (i, a), party P_0 only gains $\Theta(\frac{1}{m})$ bias. It follows that the maximal bias obtained by a fail-stop strategy for P_0 is $\Theta(\frac{1}{m})$.

Fairness via defense. Let us present a different view of the protocol of [35]. Consider a variant of this protocol without the d_i's. Namely, the parties reconstruct $c_1, \ldots, c_m$ one at a time, until they reach $c_i \neq \perp$. When an abort occurs, the remaining party outputs an unbiased coin if it has not yet reconstructed c, and outputs c otherwise. It is easy to see that an aborting attacker can bias the output of the other party in this degenerate variant by $\frac{1}{4}$; that is, it simply waits until it reconstructs c and then aborts for biasing the other party's output towards $1 - c$.

The role of "defense" values $(d_i^0, d_i^1), \ldots, (d_m^0, d_m^1)$ is to prevent such an attack; if a party aborts after reconstructing c, the other party is guaranteed to output c as well. The problem is, however, that the defense values themselves might cause a problem: a corrupted party might abort after reconstructing its defense value for the i'th round (and not only after reconstructing c_i). Indeed, by aborting in these rounds, a corrupted party does gain a bias, but only $\Theta(\frac{1}{m})$.

On extending Moran et al.'s protocol for the three-party case. We next explain why the approach of Moran et al.'s does not seem to be useful for constructing three-party fait coin0flissping protocols . [**Iftach's Note: Is it clear now?**]

In a three-party fair coin-flipping protocol, one should deal with two *non-simultaneous* aborts: after one party aborts, the remaining two parties should interact in a two-party protocol to agree on their common coin. Since one of the remaining parties might be corrupted as well, this two-party protocol needs to be a fair coin-flipping protocol as well. Moreover, the expected outcome of the latter two-party protocol, whose shares are given *before* each round, should be equal (up to an additive difference of $\Theta(\frac{1}{m})$) to the value of the three-party protocol *after* this round — the expected outcome of the protocol given the reconstructed shares. Otherwise, an aborting party can significantly bias the output of the two other parties.

Consider the following natural extension of Moran et al.'s protocol to a three-party protocol. The value of $c_1, \ldots, c_m$ are as in the two-party protocol (now shared between the three parties). The defense values are not bits, but rather two vectors of shares for the two remaining parties (different shares for each possible pair), to enable them to interact in some fair two-party coin-flipping protocol if the third party aborts.

Assume that in the i'th round of the "outer" three-party protocol, the value of c_i is one (i.e., $c_i = c = 1$), and consider the two-party protocol executed by the remaining parties, if a party aborts in this round. The outcome of the remaining party in the case of a premature abort in this underlying two-party protocol should be also one. Otherwise, two corrupted parties can mount the following two-phase attack: first aborting in the outer three-party protocol after seeing $c_i = 1$, and then prematurely aborting in the inner two-party protocol, knowing that the other party will output something that is far from one. Now, assume that in the i'th round of the "outer" three-party protocol, the value of c_i is $\perp$ (i.e., $i < i^*$), and consider again the two-party protocol executed by the remaining parties if party aborts in this round. It is easy to see that expected outcome of this two-party protocol should be close to $\frac{1}{2}$ (i.e., unbiased), and thus its defense values for the parties cannot be all the same.[**Iftach's Note: is it clear now?**]

These restrictions on the two-party protocol defense values ruin the security of the outer three-party protocol; in each round i, two corrupted (and thus colluding) parties can reconstruct the *whole* two-party execution that they should have engaged in if the other (in this case, the honest) party aborts in this round [**Iftach's Note: is it clear?**]. By checking whether the defense values of this two-party execution are all ones (indicating that $c = 1$), all zeros (indicating that $c = 0$), or mixed (indicating that $c_i = \perp$), they get enough information for biasing the output of the protocol by a constant value.

What causes the above three-party protocol to fail is that its value in a given round might be changed by $\frac{1}{2}$ (say from $\frac{1}{2}$ to 1). As we argued above, the (long) defense values reconstructed *before* each round in the three-party protocol have to contain many (i.e., m) samples drawn according to the value of the protocol at the *end* of the round. It follows that two corrupted parties might extrapolate at the *beginning* of such a round, the value of protocol when this round *ends*, thus rendering the protocol insecure. [**Iftach's Note: is it clear?**]

1.3.2 Our Smooth Two-Party Protocol

Given the above understanding, our first step is to construct a two-party coin-flipping protocol, whose value only changes *slightly* (i.e., smoothly) between consecutive rounds. In the next section we use a *derandomized* version of such a smooth coin-flipping protocol as a building block for

constructing an (almost) optimally fair three-party protocol.

Consider the $\Theta(\frac{1}{\sqrt{m}})$-bias coin-flipping protocol of Cleve [15]: in each of the m rounds, the parties reconstruct the value of a coin $c_i \in \{-1, 1\}$, and the final outcome is set to $\mathsf{sign}(\sum_{i\in[m]} c_i)$. Since the value of $\sum c_i$ is close to being uniform over $[-\sqrt{m}, \sqrt{m}]$, the value of the first coin c_1 changes the protocol's value by $\Theta(\frac{1}{\sqrt{m}})$. This sounds like a good start toward achieving a smooth coin-flipping protocol. The problem is, however, that with probability $\Theta(\frac{1}{\sqrt{m}})$, the sum of $c_1, \ldots, c_{m-1}$ is exactly zero. Hence, with this probability, the final coin changes the protocol's value by $\frac{1}{2}$.

We overcome the above problem by using a *weighted* majority protocol. In the first round the parties reconstruct m-coins (in a single shot), reconstruct $(m-1)$ coins in the second round, and so on, until in the very last round only a single coin is reconstructed. Now the value of $\sum c_i$ (now each c_i is an integer) is close to being uniform over $[-m, m]$, and the last round determines the outcome only with probability $\Theta(\frac{1}{m})$ (versus $\Theta(\frac{1}{\sqrt{m}})$ in the unweighted version). Other rounds also enjoy a similar smoothness property. We emphasize that the resulting protocol *does not* guarantee small bias (but only a $\Theta(\frac{1}{\sqrt{m}})$-bias). Rather, we take advantage of its smoothness and use it as a building block of a fair two-party protocol (and then of a three-party protocol).

The protocol. As in Moran et al. [35], the parties start by securely computing a share generating function, and then use its outputs to slowly reconstruct the output of the protocol.

Let $\mathcal{B}er(\delta)$ be the output of a coin taking the value one with probability δ and zero otherwise, let $\mathcal{B}_n$ be the sum of n uniform coins over $\{-1, 1\}$, let $\widehat{\mathsf{B}}_n(k) = \Pr_{x\leftarrow\mathcal{B}_n}[x \geq k]$, and finally, let $\mathsf{sum}(t) = t(t+1)/2 = \sum_{j\in[t]} j$.

We start by describing the share generating function and then use it to describe the protocol.

Algorithm 1.4 (share generating function $\mathsf{TwoPartySharesGen}$)**.**

1. *For $z \in \{0, 1\}$, sample $d_0^z \leftarrow \{0, 1\}$.*
2. *For $i = 1$ to $[m]$,*
   (a) *Sample $c_i \leftarrow \mathcal{B}_{m+1-i}$.*
   (b) *For $z \in \{0, 1\}$, sample $d_i^z \leftarrow \mathcal{B}er(\delta_i)$, for $\delta_i = \widehat{\mathsf{B}}_{\mathsf{sum}(m-i)}(-\sum_{j=1}^{i} c_i)$.*[3]
3. *Split each of the $3m$ values $d_1^0, d_1^1, \ldots, d_m^0, d_m^1, c_1, \ldots, c_m$ into two "shares", using a 2-out-of-2 secret sharing scheme, to create two set of shares: $\mathbf{s}^{\#\mathbf{0}}$ and $\mathbf{s}^{\#\mathbf{1}}$.*
4. *Output $(d_0^0, \mathbf{s}^{\#\mathbf{0}}), (d_0^1, \mathbf{s}^{\#\mathbf{1}})$.*

Protocol 1.5 ($\pi_2 = (\mathsf{P}_0, \mathsf{P}_1)$)**.**

Initial step: The parties securely compute the function $\mathsf{TwoPartySharesGen}$*. Let $(d_0^i, \mathbf{s}^{\#\mathbf{i}})$ be the local output of P_i.*

Main loop: For $i = 1$ to m, do

(a) *P_0 sends to P_1 its share of d_i^1, and P_1 sends to P_0 its share of d_i^0.*

[3] [**Iftach's Note: can we start a sentence with a variable name?**] δ_i is the probability that the protocol's output is one, given the value of the "coins" $c_1 \ldots, c_i$ (and assuming no abort).

- P_0 *reconstructs the value of* d_i^0*, and* P_1 *reconstructs the value of* d_i^1*.*

(b) Each party sends to the other party its share of c_i*.*

- *Both parties reconstruct the value of* c_i*.*

Output: Both parties output one if $\sum_{j=1}^{m} c_i \geq 0$*, and zero otherwise.*

Abort: If P_0 *aborts, party* P_1 *outputs the value of* d_i^1*, for the* maximal $i \in [m]$ *for which it has reconstructed this value (note that by construction such an* i *always exists).*

The case that P_1 *aborts is analogously defined.*

Namely, the parties interact in a weighted majority protocol, where in the i'th round, they reconstruct, in an unfair manner, $(m+1-i)$ coins (i.e., c_i). If a party aborts, the remaining party outputs a defense value given to it by the honest dealer (implemented via the secure computation of $\mathsf{TwoPartySharesGen}$).

A few remarks are in place. First, we will only define the protocol for $m \equiv 1 \bmod 4$. Hence, $\sum_{j=1}^{m} c_i \neq 0$, and the protocol's output is a uniform bit when played by the honest parties. Second, if P_0 aborts in the first round, the party P_1 could simply output a uniform bit. We make P_0 output d_0^1, since this be useful when the two-party protocol will be later used as part of the three-party protocol. Finally, one can define the above protocol without exposing the coins c_i's to the parties (in this case, the honest parties output (d_m^0, d_m^1) as the final outcome). We expose the coins to the parties for instructional reasons.[**Iftach's Note: what I meant that the exposing the coins make the analysis of the protocol easier to follow. Does "instructional" capture that?**]

Security of the protocol. Note that the defense value given in round (i,a) (i.e., step a of the i'th loop) is distributed according to the expected outcome of the protocol, conditioned on the value of the coin to *be given* in round (i,b). These defense values make aborting in round (i,b), for any value of i, harmless. So it is left to argue that aborting in round (i,a), for any value of i, is not too harmful either. We show that, using the fact that the value reconstructed in round (i,a) gives only a very noisy signal about the value of c_i.

Since the protocol is symmetric, we assume for concreteness that the corrupted party is P_0. Similar to the analysis of Moran et al.'s protocol sketched above, it suffices to bound the value of $|\mathsf{val}(V) - \mathsf{val}(V^-)|$.

Assume that P_0 aborts in round (i,b). By construction, $\mathsf{val}(V^-) = \delta_i$. Since, the defense of P_1 in round (i,b) is sampled according to $\mathcal{B}er(\delta_i)$, it is also the case that $\mathsf{val}(V) = \delta_i$.

Assume now that P_0 aborts in round (i,a). By construction, $\mathsf{val}(V^-) = \delta_{i-1}$. Note that V does contains some information about δ_i, i.e., a sample from $\mathcal{B}er(\delta_i)$, and thus $\mathsf{val}(V)$ is typically different from $\mathsf{val}(V^-)$. Yet, since V contains only a sample from $\mathcal{B}er(\delta_i)$, and this is a very noisy signal for the actual value of δ_i, we manage to prove the following (see Section 4 for the formal proof).

$$\left|\mathsf{val}(V) - \mathsf{val}(V^-)\right| = \frac{(\delta_i - \delta_{i-1})^2}{\delta_{i-1}}. \tag{1}$$

Equation (1) yields that $|\mathsf{val}(V) - \mathsf{val}(V^-)| = O(\frac{1}{m})$, since by the "smoothness" of the protocol (i.e., the value of the game does not change drastically between consecutive rounds) it follows that $\left|\frac{\delta_i - \delta_{i-1}}{\delta_{i-1}}\right| \in O(\frac{1}{\sqrt{m}})$ with high probability.[4]

1.3.3 Our Three-Party Protocol

We start by applying a generic approach, introduced by Beimel et al. [7], to try and extend our fair two-party protocol into a three-party one. We then explain why this generic approach does not work in our case, and show how to modify it to get a fair three-party protocol.

In the first attempted three-party protocol, the parties interact in the following variant of the two-party protocol π_2 described in Protocol 1.5. As the first step, the three parties (securely) compute the function ThreePartySharesGen, defined next, rather than TwoPartySharesGen as in protocol π_2. Let $\mathcal{B}_{n,\varepsilon}$ be the sum of n ε-biased [**Iftach's Note: each of the coin is ε-biassed (i.e., one with prob. $\frac{1}{2}+\varepsilon$). Without the hyphenation, the text is unclear)**]coins over $\{-1,1\}$ and let $\widehat{\mathsf{B}}_{n,\varepsilon}(k) = \Pr_{x \leftarrow \mathcal{B}_{n,\varepsilon}}[x \geq k]$. For $\varepsilon \in [-\frac{1}{2}, \frac{1}{2}]$, we define the function $\mathsf{TwoPartySharesGen}^{\varepsilon}$ as the following variant of the function TwoPartySharesGen defined above: (1) the "coin" c_i is sampled according to $\mathcal{B}_{m+1-i,\varepsilon}$ (and not according $\mathcal{B}_{m+1-i}$ as in TwoPartySharesGen); (2) the initial defense values d_0^0 and d_0^1 are sampled according to $\mathcal{B}er(\widehat{\mathsf{B}}_{\mathsf{sum}(m),\varepsilon}(0))$ (and not $\mathcal{B}er(\frac{1}{2}) = \mathcal{B}er(\widehat{\mathsf{B}}_{\mathsf{sum}(m)}(0))$ as in TwoPartySharesGen)

Algorithm 1.6 (share generating function ThreePartySharesGen)**.**

1. *For $i = 1$ to $[m]$,*
   (a) *Sample $c_i \leftarrow \mathcal{B}_{m+1-i}$.*
   (b) *Let $\varepsilon_i \in [-\frac{1}{2}, \frac{1}{2}]$ be the value such that $\widehat{\mathsf{B}}_{\mathsf{sum}(m),\varepsilon_i}(0) = \delta_i = \widehat{\mathsf{B}}_{\mathsf{sum}(m-i),0}(-\sum_{j=1}^{i} c_j)$.*[5]
   (c) *For each pair of the three parties, generate shares for an execution of π_2, by calling $\mathsf{TwoPartySharesGen}^{\varepsilon_i}$.*
2. *Split the values of $c_1, \ldots, c_m$ and the defense values into three set of shares using a 3-out-of-3 secret sharing scheme, and output the three sets.*

Protocol 1.7 ($\pi_3 = (\widehat{\mathsf{P}}_0, \widehat{\mathsf{P}}_1, \widehat{\mathsf{P}}_2)$)**.**

Initial step: The parties securely compute the function ThreePartySharesGen*, where each party gets one set of shares.*

Main loop: For $i = 1$ to m, do

(a) *Each party sends to the other parties its share of their defense values.*

- *Each pair $(\mathsf{P}_z, \mathsf{P}_{z'})$ of the parties reconstructs a pair of two sets of shares $d_i^{z,z'} = ((d_i^{z,z'})_z, (d_i^{z,z'})_{z'})$, to serve as input for an execution of the two-party protocol if the third party aborts (i.e., P_z reconstructs $(d_i^{z,z'})_z$, and $\mathsf{P}_{z'}$ reconstructs $(d_i^{z,z'})_{z'}$).*

[4] The $O(\log^2 m)$ factor in our actual result, was "swallowed" by the above informal arguments. [**Iftach's Note: I meant that this factor does not appear in the $O(\frac{1}{m})$, since we only gave an informal argument.**]

[5] Namely, ε_i is set to the number such that a fresh new game with ε_i-biased coins, has the same value (i.e., expected outcome) as that of the current game at this point (i.e., conditioning on $c_1, \ldots, c_i$).

(b) Each party sends the other parties its share of c_i.

- *All parties reconstruct the value of c_i.*

Output: The parties output one if $\sum_{j=1}^{m} c_i \geq 0$, and zero otherwise.

Abort:

- *If $\widehat{\mathsf{P}}_0$ aborts, the parties $\widehat{\mathsf{P}}_1$ and $\widehat{\mathsf{P}}_2$ use the shares of $d_i^{1,2}$, for the* maximal $i \in [m]$ *that has been reconstructed, to interact in π^2 (starting right after the share reconstruction phase). If no such i exists, the parties interact in the (full, unbiased) two-party protocol π^2.*

  The case that $\widehat{\mathsf{P}}_1$ or $\widehat{\mathsf{P}}_2$ aborts is analogously defined.
- *If two parties abort in the same round, the remaining party acts as if one party has only aborted in the very beginning of the two-party protocol.*

Similar to the analysis for the two-party protocol sketched above, it suffices to show that the defense values reconstructed by a pair of corrupted parties in round (i, a) — the inputs for the two-party protocols — do not give too much information about the value of δ_i — the expected outcome of the three-party protocol conditioned on the coins reconstructed at round (i, b). Note that once two corrupted parties are given these defense values, which happens in round (i, a), they can *immediately* reconstruct the whole two-party execution induced by them. This two-party execution effectively contains $\Theta(m)$ *independent* samples from $\mathcal{B}er(\delta_i)$: one sample is given explicitly as the final output of the execution, and the value of $2m$ additional samples can be extrapolated from the $2m$ defense values given to the two parties. Many such independent samples can be used to approximate the value of δ_i with accuracy $\Theta(\frac{1}{m})$. It follows that in round (i, a), two corrupted parties can rush and estimate the value of δ_i with high accuracy, and then use it to bias the outcome of the three-party protocol by $\left|\delta_i - \delta_{i-1} - \Theta(\frac{1}{m})\right| \in \Omega(\frac{1}{\sqrt{m}})$.

Derandomizing the above protocol. We handle the above problem by modifying the way the defense values given to the parties in the three-party protocol are sampled. We modify the share generating function $\mathsf{TwoPartySharesGen}^{\varepsilon}$ to first draw $\Theta(m^2)$ independent samples from $\mathcal{B}er(\varepsilon)$, and then use these samples via a simple derandomization technique for drawing the $\Theta(m)$ defense values given in the three-party protocol (see Section 3 for details). This constitute a saving in comparing to the original $\mathsf{TwoPartySharesGen}^{\varepsilon}$ which, at least for its straightforward implementation, requires $\Theta(m^3)$ (independent) samples from $\mathcal{B}er(\varepsilon)$. When called with $\varepsilon = \varepsilon_i$, the definition of ε_i yields that the information such $\Theta(m^2)$ samples contain about the value of δ_i is roughly the same as in a *constant* number of independent samples from $\mathcal{B}er(\delta_i)$. It follows that the defense values given to the parties in round (i, a) of the resulting three-party protocol, leak only a little information about the value of δ_i. This yields that a pair of colluding parties cannot bias the output of the three-party protocol by more than $\Theta(\frac{1}{m})$.

1.4 Open Problems

The existence of an optimally fair three-party coin-flipping protocol (without the $O(\log^2 m)$ factor) is still an interesting open question. A more fundamental question is whether there exists a fair coin-flipping protocol for any number of parties (against any number of corrupted parties). While constructing (at least, almost) optimally fair, m-round coin-flipping protocols for a constant (or

even $\log(m)$) number of parties seems within the reach of our current technique, handling super-logarithmic numbers of parties [**Iftach's Note: why numbers and not number?**], not to mention $\Omega(m)$, seems to require a completely new approach, an may not be possible at all.

Paper Organization

General notations and definitions used throughout the paper are given in Section 2. Our coin-flipping protocols, along with their security proofs, are given in Section 3. The proofs given in Section 3 are using tools developed in Section 4, that analyze the security of a special type of online games.[**Iftach's Note: Now?**] Missing proofs can be found in Appendix A.

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values, boldface for vectors and capital boldface for matrices. All logarithms considered here are in base two. For $a \in \mathbb{R}$ and $b \geq 0$, let $a \pm b$ stand for the interval $[a-b, a+b]$. Given sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$ and k-input function f, let $f(\mathcal{S}_1, \ldots, \mathcal{S}_k) := \{f(x_1, \ldots, x_j) \colon x_i \in \mathcal{S}_i\}$, e.g., $f(1 \pm 0.1) = \{f(x) \colon x \in [.9, 1.1]\}$.[**Iftach's Note: change '=' to $\in$**] Given a set $\mathcal{S}$ over $\{-1,1\}^*$, let $w(\mathcal{S}) = \sum_{s \in \mathcal{S}} s$. Similarly, given a vector $v \in \{-1,1\}^*$, let $w(v) = \sum_{i \in |v|} v[i]$. We let the XOR of two integers, stands for the *bitwise* XOR of their bits. For $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$ and $(n) = \{0, \ldots, n\}$. For $x \in \mathbb{R}$, let $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$.

Given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Similarly, given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution on $\mathcal{S}$. The support of a distribution D over a finite set $\mathcal{U}$, denoted $\text{Supp}(D)$, is defined as $\{u \in \mathcal{U} : D(u) > 0\}$. Given a a distribution D and set $\mathcal{S}$, let $D^{\mathcal{S}}$ be the distribution D conditioned on being in $\mathcal{S}$ (arbitrarily defined in case $\text{Supp}(D) \cap \mathcal{S} = \emptyset$). The *statistical distance* of two distributions P and Q over a finite set $\mathcal{U}$, denoted as $\text{SD}(P, Q)$, is defined as $\max_{\mathcal{S} \subseteq \mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$.

Let $n \in \mathbb{N}$, $k \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$. [**Eliad's Note: Changed!**] Let $\mathcal{B}er(\varepsilon)$ be the Bernoulli probability distribution over $\{0, 1\}$, taking the value one with probability $\frac{1}{2}(1+\varepsilon)$. Define the Binomial probability distribution $\mathcal{B}_{n,\varepsilon}$, by $\mathcal{B}_{n,\varepsilon}(k) = \Pr\left[\sum_{i=1}^{n} x_i = k\right]$, where the x_i's are i.i.d over $\{-1, 1\}$, taking the value one with probability $\frac{1}{2}(1+\varepsilon)$. Let $\widehat{\mathsf{B}}_{n,\varepsilon}(k) = \Pr_{x \leftarrow \mathcal{B}_{n,\varepsilon}}[x \geq k] = \sum_{t \geq k} \mathcal{B}_{n,\varepsilon}(t)$. For $n, n' \in \mathbb{N}$, $k \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$, let $\mathcal{B}^{-1}(n, \varepsilon, k, n')$ be the value $\varepsilon' \in [-1, 1]$ with $\widehat{\mathsf{B}}_{n',\varepsilon'}(0) = \widehat{\mathsf{B}}_{n,\varepsilon}(k)$.

Let $\ell \leq n \in \mathbb{N}$, and let $p \in [-n, n]$ be an integer. Define the hypergeometric probability distribution $\mathcal{HG}_{n,p,\ell}$, by $\mathcal{HG}_{n,p,\ell}(k) = \Pr_{\mathcal{L}}\left[\sum_{x \in \mathcal{L}} x = k\right]$, where $\mathcal{L}$ an ℓ-size set uniformly chosen from an n-size $\mathcal{S}$ over $\{-1, 1\}$, with $w(\mathcal{S}) = p$. Let $\widehat{\mathsf{HG}}_{n,p,\ell}(k) = \Pr_{x \leftarrow \mathcal{HG}_{n,p,\ell}}[x \geq k] = \sum_{t \geq k} \mathcal{HG}_{n,p,\ell}(t)$.

2.2 Multi-Party Protocols

The following discussion is restricted to no private input protocols (such restricted protocols suffice for our needs).

A k-party protocol is defined using k Touring Machines (TMs) $\mathsf{P}_1, \ldots, \mathsf{P}_k$, having the security parameter 1^κ as their common input. In each round, the parties broadcast and receive messages on a broadcast channel. At the end of protocol, each party outputs some binary string.

The parties communicate in a synchronous network, using only a broadcast channel: when a party broadcasts a message, all other parties see *the same* message. This ensures some consistency between the information the parties have. There are no private channels and all the parties see all the messages, and can identify their sender. We do not assume simultaneous broadcast. It follows that in each round, some parties might hear the messages sent by the other parties before broadcasting their messages. We assume that if a party aborts, it first broadcasts the message Abort to the other parties, and without loss of generality only does so at the end of a round in which it is supposed to send a message. A protocol is *efficient*, if its parties are PPTM, and the protocol's number of rounds is a computable function of the security parameter.

This work focuses on efficient protocols, and on malicious, static PPT adversaries for such protocols. An adversary is allowed to corrupt some subset of the parties; before the beginning of the protocol, the adversary corrupts a subset of the parties that from now on may arbitrarily deviate from the protocol. Thereafter, the adversary sees the messages sent to the corrupted parties and controls their messages. We also consider the so called *fail-stop* adversaries. Such adversaries follow the prescribed protocol, but might abort prematurely. Finally, the honest parties follow the instructions of the protocol to its completion.

2.3 The Real vs. Ideal Paradigm

The security of multiparty computation protocols is defined using the *real* vs. *ideal* paradigm [13, 21]. In this paradigm, the *real-world model*, in which protocols is executed is compared to an *ideal model* for executing the task at hand. The latter model involves a trusted party whose functionality captures the security requirements of the task. The security of the real-world protocol is argued by showing that it "emulates" the ideal-world protocol, in the following sense: for any real-life adversary A, there exists an ideal-model adversary (also known as simulator) $\mathbb{A}$ such that the global output of an execution of the protocol with A in the real-world model is distributed similarly to the global output of running Sim in the ideal model. The following discussion is restricted to random, no-input functionalities. In addition, to keep the presentation simple, we limit our attention to uniform adversaries.[6]

The Real Model. Let π be an k-party protocol and let A be an adversary controlling a subset $\mathcal{C} \subseteq [k]$ of the parties. Let $\mathrm{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa)$ denote the output of A (i.e., without loss of generality its view: its random input and the messages it received) and the outputs of the honest parties, in a random execution of π on common input 1^κ.

Recall that an adversary is *fail stop*, if until they abort, the parties in its control follow the prescribed protocol (in particular, they property toss their private random coins). We call an execution of π with such a fail-stop adversary, a fail-stop execution.

The Ideal Model. Let f be a k-output functionality. If f gets a security parameter (given in unary), as its first input, let $f_\kappa(\cdot) = f(1^\kappa, \cdot)$. Otherwise, let $f_\kappa = f$.

[6] All results stated in this paper, straightforwardly extend to the non-uniform settings.

An ideal execution of f with respect to an adversary $\mathbb{A}$ controlling a subset $\mathcal{C} \subseteq [k]$ of the "parties" and a security parameter 1^κ, denoted $\text{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)$, is the output of the adversary $\mathbb{A}$ and that of the trusted party, in the following experiment.

Experiment 2.1.

1. *The trusted party sets $(y_1, \ldots, y_k) = f_\kappa(X)$, where X us a uniform element in the domain of f_κ, and sends $\{y_i\}_{i\in\mathcal{C}}$ to $\mathbb{A}(1^\kappa)$.*
2. *$\mathbb{A}(1^\kappa)$ sends the description of a subset $\mathcal{J} \subseteq \mathcal{C}$ to the trusted party, and locally outputs some value.*
3. *The trusted party outputs $\{o_i\}_{i\in[k]\setminus\mathcal{C}}$, where o_i is equal to y_i in case $\mathcal{J} = \emptyset$, and the description of $\mathcal{J}$ otherwise.*

An adversary $\mathbb{A}$ is non-aborting, if it always sets $\mathcal{J} = \emptyset$.

2.3.1 δ-Secure Computation

The following definitions adopts the notion of δ-secure computation [8, 23, 31] for our restricted settings.

Definition 2.2 (δ-secure computation)**.** *An efficient k-party protocol π computes a k-output functionality f in a δ-*secure *manner [resp., against fail-stop adversaries], if for every $\mathcal{C} \subsetneq [k]$ and every [resp., fail-stop]* PPT *adversary* A *controlling the parties indexed by $\mathcal{C}$,*[7] *there exists a* PPT $\mathbb{A}$ *controlling the same parties, such that*

$$\text{SD}\left(\text{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa), \text{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)\right) \leq \delta(\kappa),$$

for large enough κ.

A protocol securely compute a functionality f, if it computes f in a $\text{neg}(\kappa)$-secure manner.

The protocol π computes f in a simultaneous δ-secure *manner, if the above is achieved by a* non-aborting $\mathbb{A}$*.*

Note that being simultaneous δ-secure is a very strong requirement, as it dictates that the cheating real adversary has no way to prevent the honest parties from getting their part of the output, and this should be achieved with no simultaneous broadcast mechanism.

2.4 Fair Coin-Flipping Protocols

Definition 2.3 (δ-fair coin-flipping)**.** *For $k \in \mathbb{N}$ let $\mathsf{CoinToss}_k$ be the k-output functionality from $\{0,1\}$ to $\{0,1\}^k$, defined by $\mathsf{CoinToss}(b) = b^k$. A k-party protocol π is δ-*fair coin-flipping protocol*, if it computes $\mathsf{CoinToss}_k$ in a* simultaneous δ-secure *manner.*

[7] The requirement that $\mathcal{C}$ is a *strict* subset of $[k]$, is merely for notational convinced.

2.4.1 Proving Fairness

The following lemma reduces the task of proving fairness of a coin-flipping protocol, against fail-stop adversaries, to proving the protocol is correct: the honest parties always output the same bit, and this bit is uniform in an all honest execution, and to proving the protocol is unbiased: a fail-stop adversary cannot bias the output of the honest parties by too much.

Definition 2.4 (correct coin-flipping protocols)**.** *A protocol is a* correct coin flipping*, if*

- *When interacting with an fails-stop adversary controlling a subset of the parties, the honest parties* always *output the same bit, and*
- *The common output in a random* honest *execution of π, is uniform over $\{0,1\}$.*

Given a partial view of a fail-stop adversary, we are interesting in the expected outcome of the parties, conditioned on this and the adversary making no further aborts.

Definition 2.5 (view value)**.** *Let π be a protocol in which the honest parties in always output the same bit value. For a partial aborting view v of some of the parties of π,*[8] *let $\mathsf{C}_\pi(v)$, denote the parties's view in an* honest *execution of the non-aborting parties in v, conditioned on the view of the parties whose view appear in v, and the messages of the other parties, as appear in v. Let $\mathsf{val}_\pi(v) = \mathrm{E}_{v' \leftarrow \mathsf{C}_\pi(v)}[\mathrm{out}(v')]$, where $\mathrm{out}(v')$ is the common output of the non-aborting parties in v'.*

Finally, a protocol is unbiased, if no fail-stop adversary can bias the common output of the honest parties by too much.

Definition 2.6 (unbiased coin-flipping protocols)**.** *A k-party, m-round protocol π is α-*unbiased*, if the following holds for every fail-stop adversary A controlling the parties indexed by a subset $\mathcal{C} \subset [k]$. Let V be A's view in a random execution of π in which A controls the parties indexed by $\mathcal{C}$, and let I_j be the index of the j'th round in which A sent an abort message (set to m, if no such round). Let V_i be the prefix of V at the end of the i'th round, letting V_0 being the empty view, and let V_i^- be the prefix of V_i with the i'th round abort messages (if any) removed. Then*

$$\mathop{\mathrm{E}}_{V}\left[\left|\sum_{j\in|\mathcal{C}|}\mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)\right|\right] \leq \alpha,$$

where $\mathsf{val} = \mathsf{val}_\pi$ is according to Definition 2.5.

The following is an alternative characterization of fair coin-flipping protocols (against fail-stop adversaries).

Lemma 2.7. *Let π be a correct, α-unbiased coin-flipping protocol with $\alpha(\kappa) \leq \frac{1}{2} - \frac{1}{p(\kappa)}$, for some $p \in \mathrm{poly}$. Then π is a $(\alpha(\kappa) + \mathrm{neg}(\kappa))$-secure coin-flipping protocol against fail-stop adversaries.*

Proof. Let A be a PPT fail-stop adversary controlling a subset $\mathcal{C} \subsetneq [k]$ of the parties. The ideal-world adversary $\mathbb{A}$ is defined as follows.

Algorithm 2.8 ($\mathbb{A}$)**.**

[8] I.e., a partial view of some of the parties of π, in an interaction with a fail-stop adversary.

Input: 1^κ.

Operation: Upon receiving $\{y_i = b\}_{i\in\mathcal{C}}$ *from the trusted party, for some* $b \in \{0,1\}$*, do:*

1. *Keep sampling uniformly at random coins for the parties of* π *and for* A*, on security parameter* κ*, until the honest parties' common output in the resulting execution is* b*. Abort after* $\kappa \cdot p(\kappa)$ *failed attempts.*

2. *Output* A*'s output in the above sampled execution.*

Let D_κ be the distribution of the honest parities common output, in a random execution of $\pi(1^\kappa)$, in which A controls the parties indexed by $\mathcal{C}$. Assume for a moment that the trusted party chooses its output on security parameter κ, according to D_κ (and not uniformly at random). Assume further that algorithm $\mathbb{A}$ keep sampling in Step 1. until a successful sample (and not does not attempt after for $\kappa \cdot p(\kappa)$ failed attempts). Under these assumptions, it is immediate that $\mathbb{A}$ is a *perfect* ideal variant simulator for A, i.e., $\mathrm{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa) \equiv \mathrm{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)$ for every κ. We complete the proof showing that $\mathrm{SD}(D_\kappa, U) \leq \alpha(\kappa)$, where U is the uniform distribution over $\{0,1\}$. This yields that $\mathrm{SD}\left(\mathrm{REAL}_{\pi,\mathsf{A},\mathcal{C}}(\kappa), \mathrm{IDEAL}_{f,\mathbb{A},\mathcal{C}}(\kappa)\right) \leq \alpha(\kappa)$, assuming no abort occur, where the assumption about α yields that $\mathbb{A}$ aborts only with negligible probability.

Let val, V, V_i, V_i^- and I_j be as in Definition 2.6 with respect to algorithm A, subset $\mathcal{C}$ and protocol π. We prove by induction on $\ell \in |\mathcal{C}|$ that $\mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] = \frac{1}{2} + \beta_\ell$, for $\beta_\ell = \sum_{j\in[\ell]} \mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)$. Since no abort occurs after the $|\mathcal{C}|$'th aborting round, it follows that $\mathrm{E}\left[\mathsf{val}(V)\right] = \frac{1}{2} + \beta_{|\mathcal{C}|}$. Since π is α unbiased, it follows that $\mathrm{E}\left[\mathsf{val}(V)\right] \in [\frac{1}{2} \pm \alpha(\kappa)]$, and therefore $\mathrm{SD}(D_\kappa, U) \leq \alpha(\kappa)$.

The base case (i.e., $\ell = 0$) holds by the correctness of π. Assume for $0 \leq \ell < |\mathcal{C}|$. Since no additional aborts messages were sent in $V_{I_{\ell+1}}^-$ beside the ones sent V_{I_ℓ}, it holds that

$$\mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}^-)\right] = \mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] \tag{2}$$

It follows that

$$\begin{aligned}
\mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}})\right] &= \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}^-)\right] + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \mathrm{E}\left[\mathsf{val}(V_{I_\ell})\right] + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \left(\frac{1}{2} + \sum_{j\in[\ell]} \mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-)\right) + \mathrm{E}\left[\mathsf{val}(V_{I_{\ell+1}}) - \mathsf{val}(V_{I_{\ell+1}}^-)\right] \\
&= \frac{1}{2} + \sum_{j\in[\ell+1]} \mathsf{val}(V_{I_j}) - \mathsf{val}(V_{I_j}^-).
\end{aligned}$$

The second equality holds by Equation (2), the third one by the induction hypothesis. □

2.5 Oblivious Transfer

Definition 2.9. *The* $\binom{1}{2}$ *oblivious transfer (*OT *for short) functionality, is the two-output functionality* f *over* $\{0,1\}^3$*, defined by* $f(\sigma_0, \sigma_1, i) = ((\sigma_0, \sigma_1), (\sigma_i, i))$.

Protocols the securely compute OT, are known under several hardness assumptions (cf., [3, 18, 20, 26, 30, 37]).

2.6 f-Hybrid Model

Let f be a k-output functionality. The f-hybrid model is identical to the real model of computation discussed above, but in addition, each k-size subset of the parties involved, has access to a trusted party realizing f. It is important to emphasize that the trusted party realizes f in a *non-simultaneous* manner: it sends a random output of f to the parties in an arbitrary order. When a party gets its part of the output, it instructs the trusted party to either continue sending the output to the other parties, or to send them the abort symbol (i.e., the trusted party "implements" f in a perfect non-simultaneous manner).

All notion given in Sections 2.3 and 2.4 naturally extend to the f-hybrid model, for any functionality f. In addition, the proof of Lemma 2.7 straightforwardly extends to this model.

We make use of the following known fact.

Fact 2.10. *Let f be a polynomial-time computable functionality, and assume there exists an m-round, δ-fair coin-flipping protocol in the f-hybrid model, making at most t calls to f. Assuming there exist protocols for securely computing* OT*, then there exists an $(O(t)+m)$-round, $(\delta(\kappa)+\mathrm{neg}(\kappa))$-fair coin-flipping protocol (in the real world).*

Proof. Since f be a polynomial-time computable and since we assume the existence of a protocol for securely computing OT, there exists a constant-round protocol π_f for securely computing f (cf., [32]). Let π be the m-round, δ-fair coin-flipping protocol in the f-hybrid model. Using standard techniques (see [14]), it follows that by replacing the trusted party for computing f used in π with the protocol π_f, we get an $(O(t)+m)$-round, $(\delta(\kappa)+\mathrm{neg}(\kappa))$-fair coin-flipping protocol. □

2.7 Basic Inequalities

The proofs of the following proposition, is given in Appendix A.1.

Proposition 2.11. *Let $n \in \mathbb{N}$, $\alpha > 0$, $k \in [n]$ and let $\{p_j\}_{j=k}^n$ be a set of non-negative numbers such that $\sum_{j=i}^n p_j \leq \alpha \cdot (n+1-i)$ for every $i \in \{k, k+1, \ldots, n\}$. Then, $\sum_{j=k}^n \frac{p_j}{(n+1-j)} \leq \alpha \cdot \sum_{j=k}^n \frac{1}{(n+1-j)}$.*

2.8 Facts About the Binomial Distribution

Fact 2.12 (Hoeffding's inequality for $\{-1,1\}$)**.** *Let $n, t \in \mathbb{N}$, and $\varepsilon \in [-1,1]$, then*

$$\Pr_{x \leftarrow \mathcal{B}_{n,\varepsilon}} [|x - \varepsilon n| \geq t] \leq 2e^{-\frac{t^2}{2n}}$$

Fact 2.13. *For $n \in \mathbb{N}$ and $\varepsilon \in [-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]$ it holds that $\mathrm{E}_{x \leftarrow \mathcal{B}_{n,\varepsilon}} [x^2] \leq 2n$ and $\mathrm{E}_{x \leftarrow \mathcal{B}_{n,\varepsilon}} [|x|] \leq \sqrt{2n}$.*

The proofs of the following propositions, is given in Appendix A.2.

Proposition 2.14. *Let $n \in \mathbb{N}$, $t \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$ with $|t| \leq n^{\frac{3}{5}}$, $|\varepsilon| \leq n^{-\frac{2}{5}}$ and $\frac{n+t}{2} \in \mathbb{N}$. Then*

$$\mathcal{B}_{n,\varepsilon}(t) \in (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

where $\mathsf{error} = \xi \cdot (\varepsilon^2 |t| + \frac{1}{n} + \frac{|t|^3}{n^2} + \epsilon^4 n)$ for some universal constant $\xi \geq 0$.

[**Eliad's Note: Note the change of the proposition!**]

Proposition 2.15. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $t, x, x' \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ be with $|x|, |x'|, |t| \leq c \cdot \sqrt{n \log n}$ and $|\varepsilon| \leq c \cdot \sqrt{\frac{\log n}{n}}$, for some $c \geq 1$, then*

$$\frac{\mathcal{B}_{n,\varepsilon}(t-x')}{\mathcal{B}_{n,\varepsilon}(t-x)} \in \exp\left(\frac{-2\cdot(t-\varepsilon n)\cdot x + x^2 + 2\cdot(t-\varepsilon n)\cdot x' - x'^2}{2n}\right)\cdot\left(1 \pm \varphi(c)\cdot\frac{\log^{1.5} n}{\sqrt{n}}\right).$$

Proposition 2.16. *For $n \in \mathbb{N}$, $k, k' \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$, where n is larger than a universal constant, $|k|, |k'| \leq \log(n)\cdot\sqrt{n\log n}$ and $|\varepsilon| \leq \log(n)\cdot\sqrt{\frac{\log n}{n}}$, it holds that*

$$\left|\widehat{\mathsf{B}}_{n,\varepsilon}(k) - \widehat{\mathsf{B}}_{n,\varepsilon}(k')\right| \leq \frac{|k-k'|}{\sqrt{n}}$$

Proposition 2.17. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $c, n, n' \in \mathbb{N}$, $k \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$, such that $c > 10$, $n \leq n'$, $|k| \leq c\cdot\sqrt{n\log n}$, $|\varepsilon| \leq c\cdot\sqrt{\frac{\log n}{n}}$, and $\log^{\frac{1}{2}}(n) \geq \max\{8\cdot\varphi(3c), c\}$. then $\left|\mathcal{B}^{-1}(n,\varepsilon,k,n') - \frac{\varepsilon n - k}{\sqrt{n\cdot n'}}\right| \leq \frac{\log^2 n}{\sqrt{n\cdot n'}}$.*

In the following proposition, we make use of the following notation.

Notation 2.18. *For $i, n \in \mathbb{N}$ with $i \leq n$, let $\ell_n(i) = n - i + 1$ and let $\mathsf{sum}_n(i) = \sum_{j=i}^{n}\ell_n(i) = \frac{1}{2}\cdot\ell_n(i)(\ell_n(i)+1)$.*

Proposition 2.19. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds. For every $n, i \in \mathbb{N}$, $x, \beta, \beta', \alpha, \alpha' \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ and $\mathcal{S} \subseteq \mathbb{Z}$, such that $i \leq n - \log^{1.5} n$, $|\alpha|, |\alpha'| \leq \sqrt{c\cdot\mathsf{sum}_n(i)\cdot\log n}$, $|\beta|, |\beta'| \leq \sqrt{c}$, $|x| \leq \sqrt{c\cdot\ell_n(i)\cdot\log\ell_n(i)}$, $|\varepsilon| \leq \sqrt{c\cdot\frac{\log n}{\mathsf{sum}_n(i)}}$, for some $c \geq 0$, and $\mathrm{E}_{x'\leftarrow\mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}[|x'|] \leq \mathrm{E}_{x'\leftarrow\mathcal{B}_{\ell_n(i),\varepsilon}}[|x'|]$,[9] it holds that:*

$$\mathop{\mathrm{E}}_{x'\leftarrow\mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}\left[\exp\left(\frac{\alpha\cdot x + \beta\cdot x^2 + \alpha'\cdot x' + \beta'\cdot x'^2}{\mathsf{sum}_n(i)}\right)\right] \in 1 \pm \varphi(c)\cdot\sqrt{\frac{\log n}{\ell_n(i)}}\left(1 + \frac{|x|}{\sqrt{\ell_n(i)}}\right).$$

2.9 Facts About the Hypergeometric Distribution

Fact 2.20 (Hoeffding's inequality for hypergeometric distribution)**.** *Let $\ell \leq n \in \mathbb{N}$, and $p \in \mathbb{Z}$ with $|p| \leq n$. Then*

$$\Pr_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[|x-\mu| \geq t] \leq e^{-\frac{t^2}{2\ell}}$$

where $\mu = \mathrm{E}_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[x] = \frac{\ell\cdot p}{n}$.

Proof. Immediately follows by equation (10) and (14) in [40]. □

[Eliad's Note: Change the statement and fix the proof.]

Proposition 2.21. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $p, t, x, x' \in \mathbb{Z}$ and $c \geq 0$ be such that $\left|\frac{p}{n}\right| < 1$ and $|p|, |t|, |x|, |x'| \leq c\cdot\sqrt{n\log n}$, then*

$$\frac{\mathcal{HG}_{2n,p,n}(t-x')}{\mathcal{HG}_{2n,p,n}(t-x)} \in \exp\left(\frac{-2(t-p)x + x^2 + 2(t-p)x' - x'^2}{n}\right)\cdot\left(1 \pm \varphi(c)\cdot\frac{\log^{1.5} n}{\sqrt{n}}\right).$$

[9] Recall that $X^{\mathcal{S}}$, where X is a random variable and $\mathcal{S}$ is a set, denotes a random sample according to X, conditioned on $X \in \mathcal{S}$.

3 The Protocols

The following protocols follows the high-level description given in Section 1.3.

Recall that $\mathcal{B}_{n,\varepsilon}$ is the Binomial distribution over n ε-biased $\{-1,1\}$ coins i.e., each coin is set to one with probability $\frac{1}{2}(1+\varepsilon)$,[10] and that $\widehat{\mathsf{B}}_{n,\varepsilon}(t)$ is the probability that in a random sample $x \leftarrow \mathcal{B}_{n,\varepsilon}$, it holds that $w(x) = \sum_{i\in[n]} x_i \geq t$. In addition, for $n, i \in \mathbb{N}$, let $\ell_n(i) = n+1-i$, and $\mathsf{sum}_n(i) = \sum_{j=i}^{n} \ell_n(j)$. For $\ell \in \mathbb{N}$, let $h(\ell) := \lceil \log \ell \rceil + 1$. Note that it takes ℓ bits to encode a string over $\{-1,1\}^\ell$, and $h(\ell)$ bits to encode an integer in $[-\ell, \ell]$.

3.1 Two-Party Protocol

For $z \in \{0,1\}$, let $\overline{z} = z+1 \bmod 2$.

3.1.1 The Basic Two-Party Protocol

Protocol 3.1 ($\Pi^2_m = (\mathsf{P}^2_0, \mathsf{P}^2_1)$)**.**

Common input: round parameter 1^m.

P^2_z*'s input (for* $z \in \{0,1\}$*):* $\mathbf{c}^{\#\mathbf{z}} \in \mathbb{Z}^m$ *and* $\mathbf{d}^{\mathbf{0},\#\mathbf{z}}, \mathbf{d}^{\mathbf{1},\#\mathbf{z}} \in \{0,1\}^{m+1}$.

Protocol's description:

1. *For* $i = 1$ *to* m*:*
   (a) P^2_0 *sends* $\mathbf{d}^{\mathbf{1},\#\mathbf{0}}[i]$ *to* P^2_1*, and* P^2_1 *sends* $\mathbf{d}^{\mathbf{0},\#\mathbf{1}}[i]$ *to* P^2_0.
   - *For* $z \in \{0,1\}$*, party* P^2_z *set* $d^z_i = \mathbf{d}^{\mathbf{z},\#\mathbf{0}}[i] \oplus \mathbf{d}^{\mathbf{z},\#\mathbf{1}}[i]$.

   (b) P^2_0 *sends* $\mathbf{c}^{\#\mathbf{0}}[i]$ *to* P^2_1*, and* P^2_1 *sends* $\mathbf{c}^{\#\mathbf{1}}[i]$ *to* P^2_0.
   - *Both parties set* $c_i = \mathbf{c}^{\#\mathbf{0}}[i] \oplus \mathbf{c}^{\#\mathbf{1}}[i]$.
2. *Both parties output "1" if* $\sum_{i=1}^{m} c_i \geq 0$*, and "0" otherwise.*

Abort: If the other party aborts, the remaining party P^2_z *outputs* d^z_i*, for the* maximal $i \in [m]$ *for which it has reconstructed this value. In case no such* i *exists,* P^2_z *outputs* $\mathbf{d}^{\mathbf{z},\#\mathbf{z}}[m+1]$.

To keep the above description symmetric, in Step 1a and in Step 1b, both parties are supposed to send messages. This is merely for notational convince, and one might assume that the parties send their messages in an arbitrary order.

3.1.2 Two-Party Shares Generator

Algorithm 3.2 (TwoPartySharesGen)**.**

Input: Round parameter 1^m *and* $\varepsilon \in [-1,1]$.

Operation:

1. *For* $z \in \{0,1\}$*: sample* $d^{z,\#z}_{m+1} \leftarrow \mathcal{B}er(\widehat{\mathsf{B}}_{\mathsf{sum}_m(1),\varepsilon}(0))$*. Set* $d^{z,\#\overline{z}}_{m+1}$ *arbitrarily.*
2. *For* $i = 1$ *to* m*:*

[10] Notice the slight change in notation comparing to the those used in the introduction.

(a) *Sample* $c_i \leftarrow \mathcal{B}_{\ell_m(i),\varepsilon}$.

(b) *Sample* $c_i^{\#0} \leftarrow \{0,1\}^{h(m)}$ *and set* $c_i^{\#1} = c_i \oplus c_i^{\#0}$.

(c) *For* $z \in \{0,1\}$*:*

i. *Sample* $d_i^z \leftarrow \mathcal{B}er(\widehat{\mathsf{B}}_{\mathsf{sum}_m(i+1),\varepsilon}(-\sum_{j=1}^{i} c_j))$.

ii. *Sample* $d_i^{z,\#0} \leftarrow \{0,1\}$*, and set* $d_i^{z,\#1} = d_i^z \oplus d_i^{z,\#0}$.

3. *Output* $(\mathbf{s}^{\#\mathbf{0}}, \mathbf{s}^{\#\mathbf{1}})$*, where* $\mathbf{s}^{\#\mathbf{z}} = (\mathbf{c}^{\#\mathbf{z}}, \mathbf{d}^{\mathbf{0},\#\mathbf{z}}, \mathbf{d}^{\mathbf{1},\#\mathbf{z}})$*, for* $\mathbf{c}^{\#\mathbf{z}} = (c_1^{\#z}, \ldots, c_m^{\#z})$ *and* $\mathbf{d}^{\mathbf{z},\#\mathbf{z}'} = (d_1^{z,\#z'}, \ldots, d_{m+1}^{z,\#z'})$.

3.1.3 The Final Two-Party Protocol

For $m \in \mathbb{N}$, our two-party, $3m$-round, $\frac{O(\log^2 m)}{m}$-fair coin-flipping protocol $\widehat{\Pi}^2_m$, is defined as follows.

Protocol 3.3 $(\widehat{\Pi}^2_m = (\widehat{\mathsf{P}}^2_0, \widehat{\mathsf{P}}^2_1))$**.**

Oracle: An oracle O *computing* TwoPartySharesGen.

Common input: Round parameter 1^m.

Protocol's description:

1. *The two parties using the oracle* O *to securely compute the function* $\mathsf{TwoPartySharesGen}(1^m, 0)$.[11] *Let* $\mathbf{s_0}$ *and* $\mathbf{s_1}$ *be the outputs of* $\widehat{\mathsf{P}}^2_0$*, and* $\widehat{\mathsf{P}}^2_1$ *respectively.*

2. *In case the other party aborts, the remaining party outputs a uniform coin.*

3. *Otherwise, the two parties interact in an execution of* $\Pi^2_m = (\mathsf{P}^2_0, \mathsf{P}^2_1)$*, where* $\widehat{\mathsf{P}}^2_z$ *plays the role of* P^2_z *with private input* $\mathbf{s_z}$.

3.1.4 Main Theorems for Two-Party Protocols

The following theorem states that Protocol 3.3 is an almost-optimally fair, two-party coin-flipping protocol, in the TwoPartySharesGen-hybrid model.

Theorem 3.4. *There exists* $\xi \geq 0$ *such that the following holds for any polynomial-time computable, polynomially bounded integer function* m*, with* $m(\kappa) \equiv 1 \bmod 4$ *for any* $\kappa \in \mathbb{N}$*. Let* $\widehat{\Pi}^2$ *be the protocol that on security parameter* κ*, its parties act as in protocol* $\widehat{\Pi}^2_{m(\kappa)}$ *from Protocol 3.3. Then* $\widehat{\Pi}^2$ *is a* $(2m)$*-round, two-party,* $\frac{\xi \cdot \log^2 m}{m}$*-fair, coin-flipping protocol, against unbounded fail-stop adversaries, in the* TwoPartySharesGen*-hybrid model.*

Theorem 3.4 is proven below, but we first use it to deduce an almost optimal two-party fair coin-flipping protocol, in the real (non-hybrid) model.

Theorem 3.5 (Main theorem — two-party, fair coin flipping)**.** *Assuming protocols for securely computing* OT *exist, then for any polynomially bounded, polynomial-time computable, integer function* m*, there exists an* m*-round,* $\frac{O(\log^2 m)}{m}$*-fair, two-party coin-flipping protocol.*

[11] Note that $\widehat{\mathsf{P}}^2_z$ only gets the z'th part of the output.

Proof. Define the integer function $\widetilde{m}$ by $\widetilde{m}(\kappa) = \lfloor m(\kappa)/3 \rfloor - a$, where $a \in \{0,1,2,3\}$ is the value such that $\lfloor m(\kappa)/3 \rfloor - a \equiv 1 \bmod 4$. Note that both the functionality $\mathsf{TwoPartySharesGen}(1^{\widetilde{m}(\kappa)}, 0)$ and the protocol $\widehat{\Pi}^2(1^{\widetilde{m}(\kappa)})$, are polynomial-time computable in κ, and that $\widehat{\Pi}^2(1^{\widetilde{m}(\kappa)})$ has $(2\widetilde{m}(\kappa) + O(1))$ rounds. Using information-theoretic one-time message authentication codes (cf., [35]), the functionality $\mathsf{TwoPartySharesGen}$ and protocol $\widehat{\Pi}^2$, can be compiled into functionality $\widetilde{\mathsf{TwoPartyShares}}\mathsf{Gen}$ and protocol $\widetilde{\Pi^2}$ that maintains essentially the same efficiency as the original pair, protocol $\widetilde{\Pi^2}(1^{\widetilde{m}(\kappa)})$ maintain the same round complexity, and $\widetilde{\Pi^2}(1^{\widetilde{m}(\kappa)})$ is $\left(\frac{O(\log^2 \widetilde{m}(\kappa))}{\widetilde{m}(\kappa)} + \mathrm{neg}(\kappa)\right)$-fair against *arbitrary* unbounded adversaries, in the $\widetilde{\mathsf{TwoPartyShares}}\mathsf{Gen}(1^{\widetilde{m}(\kappa)})$-hybrid model.

Assuming protocols for securely computing OT exist, Fact 2.10 yields that there exists an $(2\widetilde{m}(\kappa) + O(1))$-round, two-party, polynomial-time protocol that is $\left(\frac{O(\log^2 \widetilde{m}(\kappa))}{\widetilde{m}(\kappa)} + \mathrm{neg}(\kappa)\right)$-fair, in the *standard model*. For large enough κ, the latter protocol obtains the parameters stated in the theorem (the theorem trivially holds for small values of κ, i.e., smaller than some universal constant) □

Proving Theorem 3.4

Proof of Theorem 3.4. Fix $m = m(\kappa)$, for some $\kappa \in \mathbb{N}$. By construction, the honest parties in $\widehat{\Pi}^2_m$ always output the same bit, where under the assumption about m, it holds that $\mathsf{sum}_m(1)$, the total number of coins flipped, is odd. It follows that the common output of a random honest execution of $\widehat{\Pi}^2_m$, is a uniform bit. Namely, protocol $\widehat{\Pi}^2$ is correct according to Definition 2.4.

We assume without loss of generality that if a party aborts in the i'th round, it does so by sending the message Abort, after seeing the other party message of that round.

Let the (i,j)'th round in a random execution of $\widehat{\Pi}^2_m$, for $(i,j) \in (m) \times \{a,b\}$, stands for the j'th step of the i'th loop in the execution. Letting $(0,a)$ being the zero round, and $(0,b)$ denote the round where the "call" to $\mathsf{TwoPartySharesGen}$ is made.

Let $z \in \{0,1\}$ and let A be a fail-stop adversary controlling $\widehat{\mathsf{P}}^2_z$. Let V be $\widehat{\mathsf{P}}^2_z$'s view in a random execution of $\widehat{\Pi}^2_m$. For $\mathbf{r} = (i,j) \in (m) \times \{a,b\}$, let $V_{\mathbf{r}}$ be $\mathbf{r}$'th round prefix of V, and let $V^-_{\mathbf{r}}$ be the value of $V_{\mathbf{r}}$ with the abort message sent in the $\mathbf{r}$'th round (if any) removed. Finally, let I be the round in which A sent the abort message, letting $I = (m,b)$, in case no abort occurred.

In the following we show that

$$\mathrm{E}\left[\left|\mathsf{val}(V_I) - \mathsf{val}(V^-_I)\right|\right] \leq \frac{\xi \log^2 m}{m}, \tag{3}$$

for some universal (independent of κ) constant $\xi \geq 0$, where $\mathsf{val}(v)$ is the expected outcome of an honest (non aborting) execution of the parties that do no abort in v, conditioned on v (see Definition 2.5).

Since Equation (3) holds for any $m = m(\kappa)$ and any fail-stop adversary A, we have that protocol $\widehat{\Pi}^2$ is $\frac{\xi \log^2 m}{m}$-biassed according to Definition 2.6.[12] Since, see above, $\widehat{\Pi}^2$ is correct according to Definition 2.4, the proof of the theorem follows by Lemma 2.7.

So it is left to prove Equation (3). Notice that the next rounds shares held by $\widehat{\mathsf{P}}^2_z$ (when playing the role of P^2_z) at the end of round (i,b) (i.e., $\mathbf{c}^{\#\mathbf{z}}{}_{i+1,\ldots,m}$, $\mathbf{d}^{\mathbf{0},\#\mathbf{z}}{}_{i+1,\ldots,m+1}$ and $\mathbf{d}^{\mathbf{1},\#\mathbf{z}}{}_{i+1,\ldots,m+1}$), are uniformly chosen strings from $\widehat{\mathsf{P}}^2_z$'s point of view. In particular, these shares contains no information about the expected output of the protocol, or the other party's action in case of

[12] Equation (3) actually states that $\widehat{\Pi}^2$ is $\frac{\xi \log^2 m}{m}$-biassed even against *unbounded* adversaries.

future aborts. It follows that $\mathsf{val}(V_{0,b}) = \frac{1}{2}$ (recall that $V_{0,b}$ is $\widehat{\mathsf{P}}^2_z$'s view after getting its part of $\mathsf{TwoPartySharesGen}$'s output). We also note that by construction, in case $\widehat{\mathsf{P}}^2_z$ aborts during the "call" to $\mathsf{TwoPartySharesGen}$ (and in this case the honest party gets no value from the functionality), then the honest outputs a uniform bit. Namely, $\mathsf{val}(V^-_{(0,b)}) = \frac{1}{2}$. Hence, the adversary A gains *nothing* by aborting during the call to $\mathsf{TwoPartySharesGen}$, and in the following we assume without loss of generality that A only aborts (if any) during the execution of the embedded execution of $\Pi^2_m = (\mathsf{P}^2_0, \mathsf{P}^2_1)$.

In the rest of the proof we separately consider the case $I = (\cdot, a)$ and the case $I = (\cdot, b)$. We conclude the proof showing that the first type of aborts might help A to gain $\frac{O(\log^2 m)}{m}$ advantage, where the second type give him *nothing*.

Since both steps are symmetric, we assume for concreteness that A controls P^2_0.

$I = (\cdot, a)$. By construction, in case $I = (i, a)$, then

$$\mathsf{val}(V_I) = \mathsf{val}(V_{I-1}) = \delta_{i-1} := \widehat{\mathsf{B}}_{\mathsf{sum}_m(i),\varepsilon}\left(-\sum_{j=1}^{i-1} c_j\right),$$

letting $V_{I-1} = V_{(i-1,b)}$, where $\{c_j\}_{j\in[i-1]}$ are the coins appearing in V_{I-1}.

The view of P^2_0 has in addition to $(c_1, \ldots, c_{i-1})$ (plus some random function of them), also the value d^0_i, sampled according to $\mathcal{B}er(\delta_i)$, while the latter information might help the adversary to bias the outcome of P^2_1. By Lemma 4.4, see also Remark 4.3, the overall bias A gains from aborting in Step 1a of the loop, is bounded by $\frac{\xi \log^2 m}{m}$, for some universal constant ξ.

$I = (\cdot, b)$. In case $I = (i, b)$, the adversary's view V_I contains the value of $(c_1, \ldots, c_i)$ sampled by $\mathsf{TwoPartySharesGen}$, and some random function of these values, i.e., the shares of the next rounds it got from $\mathsf{TwoPartySharesGen}$, which are uniform strings from his point of view, and the shares used till this round, which are random function of $(c_i, \ldots, c_i)$. Hence, the expected outcome of the protocol given A's view is δ_i. By construction, however, the expected outcome of P^2_1 in case P^2_0 aborts in round (i, b), is also δ_i. Hence, the adversary gains nothing (i.e., $\mathsf{val}(V_i) = \mathsf{val}(V^-_i)$), by aborting in these steps.

□

Remark 3.6 (Intuition for the proof of Lemma 4.4)**.** *The proof of Lemma 4.4 given in Section 4 is the main technical contribution for this part. Intuitively, its correctness stems from the following observation: since c_i is the sum of $\ell_i = m + 1 - i$ uniform samples from $\{-1, 1\}$, it is unlikely that it is larger than $\sqrt{\ell_i}$. Since in the last $i-1$ rounds, $\mathsf{sum}_m(i-1) \approx \ell^2_i$ coins are flipped, their sum is close to being uniform $[-\ell_i, \ell_i]$. It follows that $\Delta_i := |\delta_i - \delta_{i-1}|$ is unlikely to be larger than $1/\sqrt{\ell_i}$. Notice that the adversary does not see δ_i at this point (otherwise, it could have biassed the outcome by Δ_i). Rather, it only sees a random sample from $\mathcal{B}er(\delta_i)$. This is a rather noisy signal, and yields that the adversary can only bias the outcome by $(\Delta_i)^2 \leq 1/\ell_i$. Since we are using weighted majority, it follows that with save but probability $i/m = 1 - \ell_i/m$, the output of the protocol is* effectively determined before *reaching the i'th round. Assume for simplicity that A only aborts, if at all, in the i'th round, for some $i \in [m]$. By the above observation, A biases the output coin by at most $\frac{\ell_i}{m} \cdot \frac{1}{\ell_i} = \frac{1}{m}$.*

3.2 Three-Party Protocol

Recall that $h(m) := \lceil \log m \rceil + 1$.

3.2.1 The Basic Three-Party Protocol

Protocol 3.7 ($\Pi^3_m = (\mathsf{P}^3_0, \mathsf{P}^3_1, \mathsf{P}^3_2)$)**.**

Common input: Round parameter 1^m.

P^3_z*'s input (for* $z \in \{0,1,2\}$*):* $\mathbf{c}^{\#\mathbf{z}} \in \{0,1\}^{m \times h(m)}$ *and* $\mathbf{D}^{(\mathbf{z}',\mathbf{z}''),\#\mathbf{z}} \in \{0,1\}^{m \times (3m+2)\cdot h(m)}$*, for all* $z' \neq z'' \in \{0,1,2\}$.

Protocol's description:

1. *For* $i = 1$ *to* m*:*

   (a) *For all* $z_s, z_r, z_o \in \{0,1,2\}$ *with* $z_r \notin \{z_s, z_o\}$*, party* $\mathsf{P}^3_{z_s}$ *sends* $\mathbf{D}^{(\mathbf{z_r},\mathbf{z_o}),\#\mathbf{z_s}}[i]$ *to* $\mathsf{P}^3_{z_r}$.

   - *For all* $z \neq z' \in \{0,1,2\}$*, party* P^3_z *sets* $\mathbf{d}_\mathbf{i}^{(\mathbf{z},\mathbf{z}')} = \bigoplus_{z'' \in \{0,1,2\}} \mathbf{D}^{(\mathbf{z},\mathbf{z}'),\#\mathbf{z}''}[i]$.

   (b) *For all* $z \in \{0,1,2\}$*, party* P^3_z *sends* $\mathbf{c}^{\#\mathbf{z}}[i]$ *to the other parties.*

   - *All parties set* $c_i = \mathbf{c}^{\#\mathbf{0}}[i] \oplus \mathbf{c}^{\#\mathbf{1}}[i] \oplus \mathbf{c}^{\#\mathbf{2}}[i]$.

Output All parties output "1" if $\sum_{i=1}^m c_i \geq 0$*, and "0" otherwise.*

Abort:

One party aborts: Let $z < z' \in \{0,1,2\}$ *be the indices of the remaining parties, and let* $i \in [m]$ *be the* maximal $i \in [m]$ *for which both* P^3_z *and* $\mathsf{P}^3_{z'}$ *have reconstructed* $\mathbf{d}_\mathbf{i}^{(\mathbf{z},\mathbf{z}')}$ *and* $\mathbf{d}_\mathbf{i}^{(\mathbf{z}',\mathbf{z})}$*, respectively. Set* i *to* $\perp$ *in case no such index exists. To decide on a common output,* P^3_z *and* $\mathsf{P}^3_{z'}$ *interact in the following two-party protocol.*

$i = \perp$*:* P^3_z *and* $\mathsf{P}^3_{z'}$ *interact in* $\widehat{\Pi}^2_m$.

$i \neq \perp$*:* P^3_z *and* $\mathsf{P}^3_{z'}$ *interact in* $\Pi^2_m = (\mathsf{P}^2_0, \mathsf{P}^2_1)$*, where* P^3_z *with input* $\mathbf{d}_\mathbf{i}^{(\mathbf{z},\mathbf{z}')}$ *plays the role of* P^2_0*, and* $\mathsf{P}^3_{z'}$ *with input* $\mathbf{d}_\mathbf{i}^{(\mathbf{z}',\mathbf{z})}$ *plays the role of* P^2_1.

Two parties abort (in the same round): Let P^3_z *be the remaining party and for an arbitrary* $z' \neq z \in \{0,1,2\}$*, let* $i \in [m]$ *be the* maximal *index for which* P^3_z *have reconstructed* $\mathbf{d}_\mathbf{i}^{(\mathbf{z}',\mathbf{z})}$*, set to* $\perp$ *in case no such index exists.*

$i = \perp$*:* P^3_z *outputs a uniform bit.*

$i \neq \perp$*: The remaining party* P^3_z *acts as if* $\mathsf{P}^3_{z'}$ *has only aborted at the very beginning of the following two-party protocol:* P^3_z *"interact" with* $\mathsf{P}^3_{z'}$ *in* $(\mathsf{P}^2_0, \mathsf{P}^2_1)$*, where* P^3_z *with input* $\mathbf{d}_\mathbf{i}^{(\mathbf{z}',\mathbf{z})}$ *plays the role of* P^2_0 *in case* $z < z'$ *and as* P^2_1 *otherwise.*[13]

Namely, at Step (a), the parties help each other to reconstruct inputs for the two-party protocol Π^2_m. More specifically, each pair of parties reconstructs two inputs (shares) for an execution of Π^2_m, one input for each party in the pair. In case a party aborts, the remaining parties use the above

[13]The latter protocol is well defined, since when aborting right at the beginning, $\mathsf{P}^3_{z'}$ does not send any message.

inputs for interacting in Π^2_m. In Step (b), the parties help each other to reconstruct the round coin (i.e., c_i).

Note that the above protocol has $4m$ rounds (in case one party abort at the end of the outer three-party protocols). While it is possible to reduce this number to $2m$ (to match the two-party case), we chose to present the somewhat simpler protocol given above.

3.2.2 Derandomized Two-Party Shares Generator

As we have mentioned in Section 1.3, we make use of a derandomized version of the two-party share generator defined above.

Algorithm 3.8 (DerTwoPartySharesGen)**.**

Input: Round parameter 1^m *and* $\varepsilon \in [-1,1]$.

Operation:

1. *For* $z \in \{0,1\}$*: sample a* $(2 \cdot \mathsf{sum}_m(1))$*-size set* $\mathcal{R}^z$ *over* $\{-1,1\}$*, where each element is independently drawn from* $\mathcal{B}er(\varepsilon)$.
2. *For* $z \in \{0,1\}$*: sample a random* $(\mathsf{sum}_m(1))$*-size subset* $\mathcal{W}^z \subset \mathcal{R}^z$*, and set* $d^{z,\#z}_{m+1}$ *to one if* $\sum_{w \in \mathcal{W}^z} w \geq 0$*, and to zero otherwise. Set* $d^{z,\#\overline{z}}_{m+1}$ *arbitrarily.*
3. *For* $i = 1$ *to* m*:*
   (a) *Sample* $c_i \leftarrow \mathcal{B}_{\ell_m(i),\varepsilon}$.
   (b) *Sample* $c^{\#0}_i \leftarrow \{0,1\}^{h(m)}$*, and set* $c^{\#1}_i = c_i \oplus c^{\#0}_i$.
   (c) *For* $z \in \{0,1\}$*:*
      i. *Sample a random* $(\mathsf{sum}_m(i+1))$*-size subset* $\mathcal{W}^z \subset \mathcal{R}^z$*, and set* d^z_i *to one if* $\sum_{j=1}^{i} c_j + \sum_{w \in \mathcal{W}^z} w \geq 0$*, and to zero otherwise.*
      ii. *Sample* $d^{z,\#0}_i \leftarrow \{0,1\}$*, and set* $d^{z,\#1}_i = d^z_i \oplus d^{z,\#0}_i$.
4. *Output* $(\mathbf{s}^{\#\mathbf{0}}, \mathbf{s}^{\#\mathbf{1}})$*, where* $\mathbf{s}^{\#\mathbf{z}} = (\mathbf{c}^{\#\mathbf{z}}, \mathbf{d}^{\mathbf{0},\#\mathbf{z}}, \mathbf{d}^{\mathbf{1},\#\mathbf{z}})$*, for* $\mathbf{c}^{\#\mathbf{z}} = (c^{\#z}_1, \ldots, c^{\#z}_m)$ *and* $\mathbf{d}^{\mathbf{z},\#\mathbf{z}'} = (d^{z,\#z'}_1, \ldots, d^{z,\#z'}_{m+1})$.

Namely, rather then sampling the defense values in Step 3.(c).i *independently* (as done in its non-derandomized variant TwoPartySharesGen), the defense values used by DerTwoPartySharesGen in the different rounds, are correlated via the sets $\mathcal{R}^0$ and $\mathcal{R}^1$ ($\mathcal{R}^z$ is used for the defense values of the party P^2_z). Note, however, that each round defense value on *its own*, has exactly the same distributed as in TwoPartySharesGen. The above derandomization plays a crucial part in the security proof of the three-party protocol given below.

3.2.3 Three-Party Shares Generator

Using the above two-party shares generator, our three-party shares generator is defined as follows.

Recall that $\mathcal{B}^{-1}(n,\varepsilon,k,n')$ is the value $\varepsilon' \in [-1,1]$ with $\widehat{\mathsf{B}}_{n',\varepsilon'}(0) = \widehat{\mathsf{B}}_{n,\varepsilon}(k)$.

Algorithm 3.9 (ThreePartySharesGen)**.**

Input: round parameter 1^m *and* $\varepsilon \in [-1,1]$.

Operation:

1. *For* $i = 1$ *to* m*:*
   (a) *Sample* $c_i \leftarrow \mathcal{B}_{\ell_m(i),\varepsilon}$.
   (b) *Sample* $(c_i^{\#0}, c_i^{\#1}) \leftarrow (\{0,1\}^{h(m)})^2$*, and set* $c_i^{\#2} = c_i \oplus c_i^{\#0} \oplus c_i^{\#1}$.
   (c) *Let* $\varepsilon_i = \mathcal{B}^{-1}(\mathsf{sum}_m(i+1), \varepsilon, -\sum_{j=1}^{i} c_i, \mathsf{sum}_m(1))$.
   (d) *For* $z < z' \in \{0,1,2\}$*:*
      i. *Sample* $(\mathbf{s_i^{(z,z')}}, \mathbf{s_i^{(z',z)}}) \leftarrow \mathsf{DerTwoPartySharesGen}(1^m, \varepsilon_i)$.[14]
      ii. *Sample* $(\mathbf{s_i^{(z,z'),\#0}}, \mathbf{s_i^{(z,z'),\#1}}, \mathbf{s_i^{(z',z),\#0}}, \mathbf{s_i^{(z',z),\#1}}) \leftarrow (\{0,1\}^{m\cdot h(m)+2(m+1)})^4$.
      Set $\mathbf{s_i^{(z,z'),\#2}} = \mathbf{s_i^{(z,z')}} \oplus \mathbf{s_i^{(z,z'),\#0}} \oplus \mathbf{s_i^{(z,z'),\#1}}$ *and* $\mathbf{s_i^{(z',z),\#2}} = \mathbf{s_i^{(z',z)}} \oplus \mathbf{s_i^{(z',z),\#0}} \oplus \mathbf{s_i^{(z',z),\#1}}$.
2. *Output* $(\mathbf{S^0}, \mathbf{S^1}, \mathbf{S^2})$*, where* $\mathbf{S^z} = (\mathbf{c^{\#z}}, \mathbf{D^{(0,1),\#z}}, \mathbf{D^{(0,2),\#z}}, \mathbf{D^{(1,0),\#z}}, \mathbf{D^{(1,2),\#z}}, \mathbf{D^{(2,0),\#z}}, \mathbf{D^{(2,1),\#z}})$*, for* $\mathbf{c^{\#z}} = (c_1^{\#z}, \ldots, c_m^{\#z})$ *and* $\mathbf{D^{(z',z''),\#z}} = (\mathbf{s_1^{(z',z''),\#z}}, \ldots, \mathbf{s_m^{(z',z''),\#z}})$.

3.2.4 The Final Three-Party Protocol

For $m \in \mathbb{N}$, our three-party, $3m$-round, $\frac{O(\log^2 m)}{m}$-fair coin-flipping protocol Π_m^3 is defined as follows.

Protocol 3.10 $(\widehat{\Pi}_m^3 = (\widehat{\mathsf{P}}_0^3, \widehat{\mathsf{P}}_1^3, \widehat{\mathsf{P}}_2^3))$**.**

Input: Round parameter 1^m.

Oracle: Oracle O_2 *and* O_3 *for computing* DerTwoPartySharesGen *and* ThreePartySharesGen *respectively.*[15]

Protocol's description:

1. *The three parties using the oracle* O_3 *to securely compute the function* $\mathsf{ThreePartySharesGen}(1^m, 0)$.[16] *Let* S_0*,* S_1*, and* S_2 *be the outputs obtained by* $\widehat{\mathsf{P}}_0^3$*,* $\widehat{\mathsf{P}}_1^3$ *and* $\widehat{\mathsf{P}}_2^3$ *respectively.*
2. *In case one party aborts, the remaining parties use oracle* O_2 *to interact in* $\widehat{\Pi}_m^2$ *(Protocol 3.3).*
3. *In case two parties aborts, the remaining party outputs a uniform bit.*
4. *Otherwise, the three parties interact in* $\Pi_m^3 = (\mathsf{P}_0^3, \mathsf{P}_1^3, \mathsf{P}_2^3)$*, where* $\widehat{\mathsf{P}}_z^3$ *plays the role of* P_z^3 *with private input* S_z.

[14] It is possible to take the derandomization a step further and reuse some of the coins flipped by DerTwoPartySharesGen. Since this change nothing asymptomatically, we chose to present this simpler approach.

[15] To be consistent with the standard hybrid model definition, which allows only a single function oracle, one can consider the function (DerTwoPartySharesGen, ThreePartySharesGen), that computes both functions simultaneously (on independent inputs).

[16] Note that $\widehat{\mathsf{P}}_z^2$ gets only z'th part of the output.

3.2.5 Main Theorems for Three-Party Protocols

Theorem 3.11. *There exists $\xi \geq 0$ such that the following holds for any polynomial-time computable, polynomially bounded integer function m, with $m(\kappa) \equiv 3 \bmod 4$ for any $\kappa \in \mathbb{N}$. Let $\widehat{\Pi}^3$ be the protocol that on security parameter κ, its parties act as in protocol $\widehat{\Pi}^3_{m(\kappa)}$ from Protocol 3.10. Then $\widehat{\Pi}^3$ is a $(4m)$-round, three-party, $\frac{\xi \cdot \log^2 m}{m}$-fair, coin-flipping protocol, against unbounded fail-stop adversaries, in the* $(\mathsf{DerTwoPartySharesGen}, \mathsf{ThreePartySharesGen})$*-hybrid model.*

As in the two-party case, we deduce the following result.

Theorem 3.12 (Main theorem — three-party, fair coin flipping)**.** *Assuming protocols for securely computing* OT *exist, then for any polynomially bounded, polynomial-time computable, integer function m, there exists an m-round, $\frac{O(\log^2 m)}{m}$-fair, three-party coin-flipping protocol.*

Proof. The only issue one should take care of in the current proof, which does not occur in the proof of Theorem 3.5, is that the function $\mathsf{ThreePartySharesGen}$ is not necessarily polynomial-time computable (even for $\varepsilon = 0$). The problem is the computing of $\varepsilon_i = \mathcal{B}^{-1}(\cdot)$, done in Step 1c. For arbitrary input parameters, perfectly calculating the output of $\mathcal{B}^{-1}$ might not be efficiently computable. Note, however, that $\mathsf{ThreePartySharesGen}$ only uses ε_i to sample $O(\mathsf{sum}_m(1)) \in \mathrm{poly}(n)$ independent samples from $\mathcal{B}er(\varepsilon_i)$. Hence, one can efficiently estimate ε_i by a value $\widetilde{\varepsilon_i}$ (say by binary search, and evaluation via sampling), such that the statistical distance of $O(\mathsf{sum}_m(1))$ independent samples from $\mathcal{B}er(\varepsilon_i)$, from $O(\mathsf{sum}_m(1))$ independent samples from $\mathcal{B}er(\widetilde{\varepsilon_i})$, is bounded by $\frac{1}{m}$. It follows that there exists a polynomial-time computable function $\widetilde{\mathsf{ThreePartySharesGen}}$, such that protocol $\widehat{\Pi}^3_m$ given in Protocol 3.10, is a $(4m)$-round, $\left(\frac{O(\log^2 m)}{m} + \frac{1}{m}\right)$-fair, three-party coin-flipping protocol, against unbounded fail-stop adversaries, in the $(\mathsf{DerTwoPartySharesGen}, \mathsf{ThreePartySharesGen})$-hybrid model. Note that using the above approximated variant of $\mathsf{ThreePartySharesGen}$, does not effect the correctness of the protocol. The proof continues like the proof of Theorem 3.5. □

Proving Theorem 3.11 We advise to reader to read first the proof of Theorem 3.4.

Proof of Theorem 3.11. As in the proof of Theorem 3.4, it holds that protocol $\widehat{\Pi}^3$ is correct according to Definition 2.4. Also as in the proof of Theorem 3.4, we assume without loss of generality that if a party aborts in the i'th round, it does so by sending the message Abort, and after seeing the other parties' message of that round.

Fix $m = m(\kappa)$, for some $\kappa \in \mathbb{N}$. Let the (p, i, j)'th round in a random execution of $\widehat{\Pi}^3_m$, for $(p, i, j) \in \{\mathsf{outer}, \mathsf{inner}\} \times (m) \times \{a, b\}$, stands for the j'th step of the i'th loop in the execution of the $\widehat{\Pi}^3_m$, where $p = \mathsf{outer}$ means that this is a step of the outer execution of $\widehat{\Pi}^3_m$, and $p = \mathsf{inner}$ means that this is a step of the inner execution of Π^2_m (whose execution starts in case a party aborts). We let $(\mathsf{outer}, 0, a)$ be the zero round, let $(\mathsf{outer}, 0, b)$ denote the round where the "call" to $\mathsf{ThreePartySharesGen}$ is made, and let $(\mathsf{inner}, 0, b)$ be the zero round in the inner execution of Π^2_m.

Let A be a fail-stop adversary controlling the parties $\{\widehat{\mathsf{P}}^3_z\}_{z \in \mathcal{C}}$, for some $\mathcal{C} \subsetneq \{0, 1, 2\}$. Let V be the view of A in a random execution of $\widehat{\Pi}^3_m$, in which A controls the parties indexed by $\mathcal{C}$. For $\mathbf{r} \in \{\mathsf{outer}, \mathsf{inner}\} \times (m) \times \{a, b\}$, let $V_{\mathbf{r}}$ be the $\mathbf{r}$'th round prefix of V, and let $V^-_{\mathbf{r}}$ be the value of $V_{\mathbf{r}}$ with the $\mathbf{r}$'th round abort messages (if any) removed. Finally, let I_1 and I_2 be the rounds in which A sent an abort message, letting $I_k = (\mathsf{outer}, m, b)$ in case less than k aborts happen. In the

following we show that for both $k \in \{1,2\}$, it holds that

$$\mathrm{E}\left[\left|\mathsf{val}(V_{I_k}) - \mathsf{val}(V^-_{I_k})\right|\right] \leq \frac{\xi \log^2 m}{m} \tag{4}$$

for some universal (independent of κ) constant $\xi \geq 0$, where $\mathsf{val}(v)$ is the expected outcome of an honest (non aborting) execution of the parties that do no abort in v, conditioned on v (see Definition 2.5. Since Equation (4) holds for any $m = m(\kappa)$ and any fail-stop adversary A, the proof of the theorem follows by Lemma 2.7.

So it is left to prove Equation (4). By construction, the only non-redundant information in A's view at the end of round (i,b) is the coins constructed by the parties at the end of this round. In particular, it holds that $\mathsf{val}(V_{\mathsf{outer},0,b}) = \frac{1}{2}$. By construction, in case two parties abort during the "call" to $\mathsf{ThreePartySharesGen}$, the remaining party outputs one with probability $\frac{1}{2}$. In case one party aborts, the remaining parties interact in the unbiased protocol $\widehat{\Pi}^2_m$. In both cases, it holds that $\mathsf{val}(V^-_{\mathsf{outer},0,b}) = \frac{1}{2}$. Taken the security of protocol $\widehat{\Pi}^2_m$ (proven in Theorem 3.4) into account, we can assume without loss of generality that A only aborts (if any) during the embedded execution of $\Pi^3_m = (\widehat{\mathsf{P}}_0, \widehat{\mathsf{P}}_1, \widehat{\mathsf{P}}_2)$.

In the rest of the proof we separately bound the case $k = 1$ and $k = 2$. Note that I_1 is of the form $(\mathsf{outer}, \cdot, \cdot)$, where I_2, unless equals (outer, m, b), is of the form $(\mathsf{inner}, \cdot, \cdot)$ (i.e., the first abort is in the outer three-party protocol, and the second, if any, is in the inner two-party protocol.).

First abort. We separately consider the case $I_1 = (\mathsf{outer}, \cdot, a)$ and the $I = (\mathsf{outer}, \cdot, b)$. We conclude the proof, of this part, showing that the first type of aborts might help A to gain $\frac{O(\log^2 m)}{m}$ advantage, where the second type give him *nothing*.

$I_1 = (\mathsf{outer}, \cdot, a)$. Assume that $I_1 = (\mathsf{outer}, i, a)$ for some $i \in [m]$. By construction,

$$\mathsf{val}(V_{I_1}) = \mathsf{val}(V_{I_1-1}) = \widehat{\mathsf{B}}_{\mathsf{sum}_m(i),0}\left(-\sum_{j=1}^{i-1} c_j\right), \tag{5}$$

letting $V_{I_1-1} = V_{(\mathsf{outer},i-1,b)}$, where $\{c_j\}_{j\in[i-1]}$ are the coins appearing in V_{I_1-1}.

Assume two parties abort in I_1'th round, and let $\{z, z'\} = \mathsf{C}$. Hence, in addition to $\{c_j\}_{j\in[i-1]}$ (and some random function of this values), view V_{I_1} contains the vectors $\mathbf{d}_{\mathbf{i}}^{(\mathbf{z},\mathbf{z}')}$ and $\mathbf{d}_{\mathbf{i}}^{(\mathbf{z}',\mathbf{z})}$, and two bit values $(\mathbf{d}_{\mathbf{i}}^{(\mathbf{z},\mathbf{z}'')})_{m+1}$ and $(\mathbf{d}_{\mathbf{i}}^{(\mathbf{z}',\mathbf{z}'')})_{m+1}$, where $\widehat{\mathsf{P}}_{z''}$ is the remaining honest party. In turn, these vectors are a random function of $9 \cdot \mathsf{sum}_m(1)$ independent samples according to $\varepsilon_i = \mathcal{B}^{-1}(\mathsf{sum}_m(i+1), 0, -\sum_{j=1}^{i} c_i, \mathsf{sum}_m(1))$, sampled in the calls to $\mathsf{DerTwoPartySharesGen}$ done by $\mathsf{ThreePartySharesGen}$.[17] Lemma 4.6 tells us (see also Remark 4.3) that if V_{I_1} would have contained *exactly* the values of $\{c_j\}_{j\in[i-1]}$ and the above $9 \cdot \mathsf{sum}_m(1)$ samples (and nothing else), then

$$\mathrm{E}\left[\left|\mathsf{val}(V^-_{I_1}) - \mathsf{val}(V_{I_1-1})\right|\right] \leq \frac{\xi_1 \log^2 m}{m} \tag{6}$$

[17] $(\mathbf{d}_{\mathbf{i}}^{(\mathbf{z},\mathbf{z}')}, \mathbf{d}_{\mathbf{i}}^{(\mathbf{z}',\mathbf{z})})$ is the output of $\mathsf{DerTwoPartySharesGen}$ which is a random function of $5 \cdot \mathsf{sum}_m(1)$ independent samples: $2 \cdot \mathsf{sum}_m(1)$ for each party's defence values and $\mathsf{sum}_m(1)$ samples for generating the values of $c_1, \ldots, c_m$. In addition, each of the two bits $(\mathbf{d}_{\mathbf{i}}^{(\mathbf{z},\mathbf{z}'')})_{m+1}$ and $(\mathbf{d}_{\mathbf{i}}^{(\mathbf{z}',\mathbf{z}'')})_{m+1}$ is a random function of $2 \cdot \mathsf{sum}_m(1)$ independent samples. Thus, in addition to $\{c_j\}_{j\in[i-1]}$, the view V_{I_1} contains a random function of $9 \cdot \mathsf{sum}_m(1)$ independent samples.

for some universal constant ξ_1. Using Proposition 4.7, it follows that the latter holds also in case $V_{I_1}^-$ contains a random function of the above value. Namely, Equation (6) holds also without the above assumption. Furthermore, the same reasoning yields that Equation (6) holds also in case the number of aborting parties in the I_1 round is one.

$I_1 = (\mathsf{outer}, \cdot, b)$ Assume that $I_1 = (\mathsf{outer}, i, b)$ for some $i \in [m]$. The view of A at this point (i.e., V_{I_1}) contains the value of $(c_1, \ldots, c_i)$, and some random function of these values. Hence, $\mathsf{val}(V_{I_1}^-) = \delta_i := \widehat{\mathsf{B}}_{\mathsf{sum}_m(i+1),0}\left(-\sum_{j=1}^{i} c_j\right)$. By construction, δ_i is also the expected outcome of the remaining parties, in case an abort message was sent in this round. Namely, $\mathsf{val}(V_i) = \delta_i$. Hence, the adversary gains nothing (i.e., $\mathsf{val}(V_i) = \mathsf{val}(V_i^-)$), by aborting in this round.

Second abort. We assume without loss of generality that $I_2 = (\mathsf{inner}, \cdot, \cdot)$ (i.e., a second abort occurred). Assume $I_1 = (\mathrm{out}, j, \cdot)$ and let ε be the value of ε_j computed by $\mathsf{ThreePartySharesGen}$, for generating the shares of the two-party protocol (via calling to $\mathsf{DerTwoPartySharesGen}$). In case $|\varepsilon| \geq 4\sqrt{\frac{\log m}{\mathsf{sum}_m(m)}}$, then by Hoeffding bound it holds that $\mathsf{val}(V_{(\mathsf{inner},0,b)}) \notin [\frac{1}{m^2}, 1 - \frac{1}{m^2}]$. In this case, Proposition 4.8 yields that the adversary cannot bias the outcome of the inner protocol, by more than $\frac{1}{m}$. Thus, in the following we can safely assume that $|\varepsilon| < 4\sqrt{\frac{\log m}{\mathsf{sum}_m(m)}}$.

The following proof is similar to analysis of the two-party protocol Π_m^2, done in the proof of Theorem 3.4, but with few differences. We separately consider the case $I_2 = (\mathsf{inner}, \cdot, a)$ and the case $I_2 = (\mathsf{inner}, \cdot, b)$. We conclude the proof showing that the first type of aborts might help A to gain $\frac{O(\log^2 m)}{m}$ advantage, where the second type give him *nothing*.

$I_2 = (\mathsf{inner}, \cdot, a)$. By construction, in case $I_2 = (\mathsf{inner}, i, a)$, it holds that

$$\mathsf{val}(V_{I_2}) = \mathsf{val}(V_{I_2-1}) = \widehat{\mathsf{B}}_{\mathsf{sum}_m(i),\varepsilon}\left(-\sum_{j=1}^{i-1} c_j\right), \tag{7}$$

letting $V_{I_2-1} = V_{(\mathsf{inner},i-1,b)}$, where $\{c_j\}_{j\in[i-1]}$ are the coins appearing in V_{I_2-1}. The view $V_{I_2}^-$ contains in addition to the coins $(c_1, \ldots, c_{i-1})$ (plus some random function of them), also the view of the outer protocol, and the bit d_i^1. The latter bit is set to one, if $\sum_{j=1}^{i} c_j + \sum_{w\in\mathcal{W}^z} w \geq 0$, and to zero otherwise, where $\mathcal{W}$ is a random $(\mathsf{sum}_m(i+1))$-size subset of the $(2 \cdot \mathsf{sum}_m(1))$-size set $\mathcal{R}^z$, sampled by $\mathsf{DerTwoPartySharesGen}$ (letting z be the index of the corrupted party in this two-party execution). In other words, d_i^1 is sampled according to

$$\mathcal{B}er\left(\widehat{\mathsf{HG}}_{2\cdot\mathsf{sum}_m(1),w(\mathcal{R}^z),\mathsf{sum}_m(i+1)}\left(-\sum_{j=1}^{i} c_j\right)\right), \tag{8}$$

where $\widehat{\mathsf{HG}}_{n,p,\ell}(k) = \Pr_{x\leftarrow\mathcal{HG}_{n,p,\ell}}[x \geq k]$, $\mathcal{HG}_{n,p,\ell}$ is the hypergeometric probability distribution (see Section 2.1), and $w(\mathcal{R}) = \sum_{r\in\mathcal{R}} r$.

Since by assumption $|\varepsilon| < 4\sqrt{\frac{\log m}{\mathsf{sum}_m(1)}}$, by Hoeffding bound it holds that $\Pr\left[|w(\mathcal{R}^z)| > 32\sqrt{\log(\mathsf{sum}_m(1)) \cdot \mathsf{sum}_m(1)}\right] \leq \frac{1}{\mathsf{sum}_m(1)} \leq \frac{2}{m^2}$. Hence, we can safety assume that $|w(\mathcal{R}^z)| \leq 32\sqrt{\log(\mathsf{sum}_m(1)) \cdot \mathsf{sum}_m(1)}$.

Given the above, Lemma 4.5 tells us that if $V^-_{I_2}$ would have contained exactly the values of $\{c_j\}_{j\in[i-1]}$, the bit d^1_i and the set $\mathcal{R}^z$ (which does not explicitly appear in $V^-_{I_2}$), then

$$\mathrm{E}\left[\left|\mathsf{val}(V^-_{I_2}) - \mathsf{val}(V_{I_2-1})\right|\right] \leq \frac{\xi_2(32)\cdot\log^2 m}{m} \tag{9}$$

for some universal function (independent of m and ε) ξ_2. Using Proposition 4.7, it follows that the latter holds also in case $V^-_{I_2}$ contains a random function of the above value. In particular, Equation (6) holds also without the above unrealistic assumption.

$I_2 = (\mathsf{inner}, \cdot, b)$. Assume $I_2 = (\mathsf{inner}, i, b)$. The view of A at this point (i.e., V_{I_2}) contains the value of $(c_1, \ldots, c_i)$ sampled by $\mathsf{DerTwoPartySharesGen}$, and some random function of these values. Hence,

$$\mathsf{val}(V^-_{I_1}) = \delta_i := \widehat{\mathsf{B}}_{\mathsf{sum}_m(i+1),\varepsilon}\left(-\sum_{j=1}^{i} c_j\right)$$

By construction, δ_i is also the expected outcome of the remaining party, in case an abort message was sent in this round. It follows that $\mathsf{val}(V_i) = \delta_i$, and the adversary gains nothing (i.e., $\mathsf{val}(V_i) = \mathsf{val}(V^-_i)$), by aborting in this round.

The above point needs is somewhat subtle and deserves some justification. Note that the output of the remaining party P^2_z is not directly sampled from $\mathcal{B}er(\delta_i)$, as in the case of protocol $\widehat{\Pi}^2_m$ considered in the proof of Theorem 3.4. Rather, a $(2\cdot\mathsf{sum}_m(1))$-size set $\mathcal{R}^z$ is sampled according to $\mathcal{B}er(\varepsilon)$ (see Algorithm 3.8). Then, the output of the remaining party is set to one if $\sum_{j=1}^{i} c_j + \sum_{w\in\mathcal{W}^z} w \geq 0$, and to zero otherwise, where $\mathcal{W}$ is random $(\mathsf{sum}_m(i+1))$-size subset of $\mathcal{R}^z$. Yet, it is easy to verify that the resulting output distribution of the remaining party is $\mathcal{B}er(\delta_i)$.[18] □

4 Bounds for Online Weighted Binomial Games

In an online binomial game, binomial random variables $X_1, \ldots, X_n$ over $\{-1, 1\}$ are independently sampled, and the value of the game is set to one if $\sum X_i \geq 0$, and to zero otherwise. At the i'th round of the game, the value of X_i is exposed to an (unbounded) attacker, who is also getting some auxiliary information about the value of X_{i+1}. The attacker can abort, and in this case it gets the expected value of the game, conditioned on the value of $X_1, \ldots, X_i$ (but not on the additional information). If no abort occurred, the attacker is getting the final value of the game. The goal of the attacker is to bias the value it gets *away* from the expected value of the game.

We are concerned with the weighted version of the above online game, in which the samples of X_i for small value of i, effects the expected outcome of the game more significantly than a sample of X_i with higher value of i. Such games are less vulnerable to a "wait for the last round" attack; attackers that wait for the very last round, and then (using the fact that the final outcome of the game is almost determined), mount a successful attack. Below we formally define such online weighted binomial games, and state our bounds for the game values of three instantiations of this game (with respect to different auxiliary information given to the attacker).

[18] This weird form of sampling from $\mathcal{B}er(\delta_i)$, was needed for the security of the outer three party protocol $\widehat{\Pi}^3_m$. We also note that unlike in protocol $\widehat{\Pi}^2_m$, the output in case of abort of party P^2_1 in the different rounds, is *not* independent (all functions of the same set $\mathcal{R}$). As noticed above, this dependency does not effect the above analysis.

4.1 Online Weighted Binomial Game

In the following we let $\ell_n(i) = n+1-i$, and let $\mathsf{sum}_n(i) = \sum_{j=i}^{n} \ell_n(i) = \frac{1}{2} \cdot \ell_n(i)(\ell_n(i)+1)$. Recall that $[i] = \{1, \ldots, i\}$ and $(i) = \{0, 1, \ldots, i\}$.

Definition 4.1 (online weighted binomial game)**.** *Given a randomized function f, integer $n \in \mathbb{N}$, $m \in \mathbb{Z}$ and constant $\varepsilon \in [-1,1]$, the* online game $\mathsf{G}_{f,n,\varepsilon,m}$ *is defined as the set of the following random variables. Let $Y_0 = X_0 = m$, and for $i \in [n]$, let*

- *X_i is sampled from $\mathcal{B}_{\ell_n(i),\varepsilon}$.*
- *$A_i = f(i, Y_i)$, for $Y_i = \sum_{\ell=1}^{i} X_\ell$.*

In addition, for $i \in [n]$, $k \in \mathbb{Z}$ and $a \in \mathcal{D}(f)$, let $V_i = \Pr[Y_n \geq 0 \mid Y_i]$, $V_{i|k} = \Pr[Y_n \geq 0 \mid Y_i = k]$ and $V_{i|k,a} = \Pr[Y_n \geq k \mid Y_i = k, A_{i+1} = a]$. Finally, let $\mathsf{G}_{f,n,\varepsilon} = \mathsf{G}_{f,n,\varepsilon,0}$

Namely, $V_{i|k}$ is the expected output of the game, conditioned on $Y_i = k$, where $V_{i|k,a}$ is the expected output of the game, conditioned on $Y_i = k$ and $A_{i+1} = a$.

Definition 4.2 (game value)**.** *The* (online) value *of the game $\mathsf{G}_{f,n,\varepsilon,m}$ with respect to a* strategy B*, is defined as*

$$\mathsf{val}_{\mathsf{B}}(\mathsf{G}_{f,n,\varepsilon,m}) = \mathrm{E}\left[\left|V_{I|Y_I,A_{I+1}} - V_{I|Y_I}\right|\right],$$

where $I = I(\mathsf{G}_{f,n,\varepsilon,m}, \mathsf{B})$ is the first $i \in [n]$ such that $\mathsf{B}(i, Y_i, A_{i+1}) = 1$, letting $I = 0$, if no such i exists.

The value *of $\mathsf{G}_{f,n,\varepsilon,m}$, is defined as $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon,m}) = \max_{\mathsf{B}}\{\mathsf{val}_{\mathsf{B}}(\mathsf{G}_{f,n,\varepsilon,m})\}$, where the maximum is over* all *possible strategies B.*

Remark 4.3 (extensions)**.** *In Section 3 we consider games in which the adversary gets in addition to Y_i and A_{i+1}, also a random function of Y_i. It is clear that any bound for the game defined above, also applied for such games.*

We also consider games in which the adversary is restricted to abort only in some apriority given set of rounds. We naturally apply the bounds below for such games, by concatenating the values it get in the non-aborting rounds with the value of the next round in which it is allowed to abort.

We give upper bounds for the security of three different types of online weighted binomial games, which we call *simple*, *hypergeometric* and *vector* games.

Lemma 4.4 (simple game)**.** *There exists $\xi > 0$ such that the following holds. Let $n \in \mathbb{N}$, let $\varepsilon \in [-1,1]$ and let f be the randomized function that on input (i,k) outputs 1 with probability $V_{i|k}$ $(= \widehat{\mathsf{B}}_{\mathsf{sum}_n(i+1),\varepsilon}(-k))$, and zero otherwise. Then $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon}) \leq \frac{\xi \cdot \log^2 n}{n}$.*

Lemma 4.5 (hypergeometric game)**.** *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds. Let $n \in \mathbb{N}$, let $p \in \mathbb{Z}$, let $\varepsilon \in [-1,1]$ and let f be the randomized function that on input (i,k), outputs 1 with probability $\widehat{\mathsf{HG}}_{2\cdot\mathsf{sum}_n(1),p,\mathsf{sum}_n(i+1)}(-k)$ and zero otherwise. Assume that $|p| \leq \gamma \cdot \sqrt{\log n \cdot \mathsf{sum}_n(1)}$ for some $\gamma > 0$, then $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon}) \leq \frac{\varphi(\gamma) \cdot \log^2 n}{n}$.*

Namely, in the above game the value of f is not sampled according to the value of the game, as done in the simple game above, but rather from a skewed version of it, obtained by replacing the Binomial distribution used by the game, with an Hypergeometric distribution.

Lemma 4.6 (vector game)**.** *There exists $\xi > 0$ such that the following holds. Let $n \in \mathbb{N}$, and let f be the randomized function that on input (i,k), outputs a string in $\{-1,1\}^{9\cdot\mathsf{sum}_n(1)}$, where each of entries takes the value 1 with probability $\mathcal{B}^{-1}(\mathsf{sum}_n(i+1),0,-k,\mathsf{sum}_n(1))$. Then $\mathsf{val}(\mathsf{G}_{f,n,0}) \leq \frac{\xi\cdot\log^2 n}{n}$.* [19]

In the last game, the function f out a vector (i.e., a string), and not a bit as in the pervious games. The distribution from which the vector is drawn, however, is very related to the value of the game.

The proof of the above lemmas are given in Sections 4.3 to 4.5, but we first develop some basic tools for analyzing Binomial games. In the following we assume that n is larger than some universal constant (for small n's, the above lemmas hold trivially).

4.2 Bounding Game Value — Basic Tools

We present three useful tools for bounding a game value.

Proposition 4.7. *For functions f and g, integer $n \in \mathbb{N}$, $m \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$, let $\mathsf{G}_{f,n,\varepsilon,m}$ and $\mathsf{G}_{g\circ f,n,\varepsilon,m}$ be a game according to Definition 4.1. Then $\mathsf{val}(\mathsf{G}_{g\circ f,n,\varepsilon,m}) \leq \mathsf{val}(\mathsf{G}_{f,n,\varepsilon,m})$.*

Proof. [**Eliad's Note: check this proof with Iftach**] Let Y_i be as in Definition 4.1 with respect to n and ε, and let $h = g \circ f$. Assume that $\mathsf{val}(\mathsf{G}_{h,n,\varepsilon,m}) = \delta$, let B_h be the strategy that realizes this value and let B_f be the strategy that on input (i,a), outputs one iff $\mathsf{B}_h(i,f(a))$ outputs one. Let I be the first output on which B_h outputs one in $\mathsf{G}_{h,n,\varepsilon,m}$. It follows that

$$\begin{aligned}
\mathsf{val}(\mathsf{G}_{h,n,\varepsilon,m}) &= \mathsf{val}_{\mathsf{B}_h}(\mathsf{G}_{h,n,\varepsilon,m}) \\
&= \mathop{\mathrm{E}}_{i\leftarrow I}\left[\left|\mathop{\mathrm{E}}_{y\leftarrow Y_{i-1},a\leftarrow h(i,Y_i)|I=i}\left[\Pr\left[Y_n \geq 0 \mid Y_{i-1}=y, h(i,Y_i)=a\right] - \Pr\left[Y_n \geq 0 \mid Y_{I-1}=y\right]\right]\right|\right] \\
&\leq \mathop{\mathrm{E}}_{i\leftarrow I}\left[\left|\mathop{\mathrm{E}}_{y\leftarrow Y_{i-1},a\leftarrow f(i,Y_i)|I=i}\left[\Pr\left[Y_n \geq 0 \mid Y_{i-1}=y, f(i,Y_i)=a\right] - \Pr\left[Y_n \geq 0 \mid Y_{I-1}=y\right]\right]\right|\right] \\
&= \mathsf{val}_{\mathsf{B}_f}(\mathsf{G}_{f,n,\varepsilon,m}) \\
&\leq \mathsf{val}(\mathsf{G}_{f,n,\varepsilon,m}).
\end{aligned}$$

The first inequality holds by the triangle inequality (for the L_1 norm), and the before to last equality holds, since I also describes the first output on which B_f outputs one in $\mathsf{G}_{f,n,\varepsilon}$ (i.e., the output of B_h and B_f in the i'th round, is the *same* random function of Y_{i-1} and Y_i, i.e., $\mathsf{B}_h(i,Y_{i-1},h(i,Y_i))$ and $\mathsf{B}_h(i,Y_{i-1},g\circ f(i,Y_i))$, respectively. □

Proposition 4.8. *Let $\mathsf{G}_{f,n,\varepsilon,m}$ and V_0 be as in Definition 4.1. Assume that $V_0 \notin [\frac{1}{n^2}, 1-\frac{1}{n^2}]$, then $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon,m}) \leq \frac{2}{n}$.*

Proof. We prove the case $V_0 \leq \frac{1}{n^2}$, where the other case is analogues. By a simple averaging argument, it holds that

$$\Pr\left[\exists i \in [n+1] \colon V_i > \frac{1}{n}\right] \leq \frac{1}{n} \tag{10}$$

[19] The constant 9 appearing in the term $9\cdot\mathsf{sum}_n(1)$ is arbitrary, and the statement holds, with a different constant ξ, for any integer.

Consider the game $\mathsf{G}_{g,n,\varepsilon,m}$ for $g(i,k)=k$. By the above, $\mathsf{val}(\mathsf{G}_{h,n,\varepsilon,m}) \leq \frac{2}{n}$. Hence, Proposition 4.7 yields that the same also holds for $\mathsf{G}_{f,n,\varepsilon,m}$. □

The above proposition states that when a game value is almost determined, there is mo much room for an attacker to gain much.

The following lemma is the main tool developed in this section, and an important role in the proofs of Lemmas 4.4 to 4.6.

Definition 4.9. *For $n \in \mathbb{N}$, $i \in (n-1)$ and $\varepsilon \in [-1,1]$, let $\mathcal{U}_{n,i,\varepsilon} = \{k \in Z\colon |k + \varepsilon \cdot \mathsf{sum}_n(i+1)| \leq \sqrt{8 \cdot \log(n) \cdot \mathsf{sum}_n(i+1)}\}$.* [20]

Proposition 4.10. *Let $\mathsf{G}_{f,n,\varepsilon,m}$, $\{X_i\}_{i\in(n)}$ be as in Definition 4.1, let $i \in (n-1)$ and let $Z_i = \sum_{\ell=i+1}^{n} X_\ell$. Then, for every $k \in \mathbb{Z}$ such that $k \notin \mathcal{U}_{n,i,\varepsilon}$ it holds that $\Pr[Z_i + k \geq 0] \notin (\frac{1}{n^2}, 1-\frac{1}{n^2})$.*

Proof. Assume $k + \varepsilon \cdot \mathsf{sum}_n(i+1) \leq 0$, where proving the case $k + \varepsilon \cdot \mathsf{sum}_n(i+1) > 0$ is analogous. Since $k \notin \mathcal{U}_{n,i,\varepsilon}$ it holds that $-(k + \varepsilon \cdot \mathsf{sum}_n(i+1)) > \sqrt{8 \cdot \log(n) \cdot \mathsf{sum}_n(i+1)}$. Note that $\mathrm{E}[Z_i] = \varepsilon \cdot \mathsf{sum}_n(i+1)$ since Z_i is distributed according to $\mathcal{B}_{\mathsf{sum}_n(i+1),\varepsilon}$. Therefore, by Hoeffding's inequality (Fact 2.12) it follows that

$$\begin{aligned} &\Pr[Z_i + k \geq 0] \\ &\quad = \Pr[Z_i - \varepsilon \cdot \mathsf{sum}_n(i+1) \geq -(k + \varepsilon \cdot \mathsf{sum}_n(i+1))] \\ &\quad \leq \Pr\left[Z_i - \varepsilon \cdot \mathsf{sum}_n(i+1) \geq \sqrt{8 \cdot \log(n) \cdot \mathsf{sum}_n(i+1)}\right] \\ &\quad \leq \frac{1}{n^2} \end{aligned} \tag{11}$$

□

Definition 4.11. *For $n \in \mathbb{N}$, $i \in (n-1)$ and $\varepsilon \in [-1,1]$, let $\mathcal{X}_i = \{x \in \mathbb{Z}\colon |x| \leq 2\sqrt{\ell_n(i+1)\log \ell_n(i+1)}\}$.* [21]

Proposition 4.12. *Let $\mathsf{G}_{f,n,\varepsilon,m}$, $\{X_i\}_{i\in(n)}$* [**Eliad's Note: check the $i \in (n-1)$ in all the places**] *be as in Definition 4.1, and assume $|\varepsilon| \leq 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}$. Then, for every $i \in (n - \log^{1.5} n)$, the following inequalities holds.*

1. $\Pr[X_{i+1} \notin \mathcal{X}_i] \leq \frac{1}{\ell_n(i+1)}$,
2. $\mathrm{E}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[|x|] < \mathrm{E}_{x \leftarrow X_{i+1}}[|x|]$,[22]
3. $\mathrm{E}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[x^2] < \mathrm{E}_{x \leftarrow X_{i+1}}[x^2]$.

[20] The constant $\sqrt{8}$ is large enough for Proposition 4.10 to hold.

[21] The constant 2 is large enough for Item 1 of Proposition 4.12 to hold.

[22] Recall that $X^{\mathcal{S}}$, where X is a random variable and $\mathcal{S}$ is a set, denotes a random sample according to X, conditioned on $X \in \mathcal{S}$.

Proof. For proving Item 1, note that the bound of $|\varepsilon|$ yields that $\mathrm{E}[X_{i+1}] = \varepsilon \cdot \ell_n(i+1) \in (-8\sqrt{\log n}, 8\sqrt{\log n})$. Therefore, by Hoeffding's inequality (Fact 2.12) it follows that [**Eliad's Note: give lower bound on n, maybe $n \geq 2^{16}$**]

$$\begin{aligned}
&\Pr[X_{i+1} \notin \mathcal{X}_i] \\
&\quad = \Pr\left[|X_{i+1}| > 2\sqrt{\ell_n(i+1)\log \ell_n(i+1)}\right] \\
&\quad \leq \Pr\left[\left|X_{i+1} - \mathrm{E}[X_{i+1}]\right| > 1.5 \cdot \sqrt{\ell_n(i+1)\log \ell_n(i+1)}\right] \\
&\quad \leq \frac{1}{\ell_n(i+1)}
\end{aligned} \tag{12}$$

Next, we will prove Item 2, where the proof of Item 3 is analogous. Compute

$$\begin{aligned}
\mathop{\mathrm{E}}_{x \leftarrow X_{i+1}}[|x|] &= \Pr_{x \leftarrow X_{i+1}}[X_{i+1} \in \mathcal{X}_i] \cdot \mathop{\mathrm{E}}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[|x|] + \Pr_{x \leftarrow X_{i+1}}[X_{i+1} \notin \mathcal{X}_i] \cdot \mathop{\mathrm{E}}_{x \leftarrow X_{i+1}^{\neg\mathcal{X}_i}}[|x|] \\
&> \Pr_{x \leftarrow X_{i+1}}[X_{i+1} \in \mathcal{X}_i] \cdot \mathop{\mathrm{E}}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[|x|] + \Pr_{x \leftarrow X_{i+1}}[X_{i+1} \notin \mathcal{X}_i] \cdot \mathop{\mathrm{E}}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[|x|] \\
&= \mathop{\mathrm{E}}_{x \leftarrow X_{i+1}^{\mathcal{X}_i}}[|x|].
\end{aligned} \tag{13}$$

□

[**Eliad's Note: note the bound of $|\varepsilon|$**]

Definition 4.13 (ratio function)**.** *Let $\mathsf{G}_{f,n,\varepsilon,m}$, $\{X_i\}_{i\in(n)}$, $\{Y_i\}_{i\in(n)}$ and $\{A_i\}_{i\in(n)}$ be as in Definition 4.1, defined the function $\mathsf{ratio} = \mathsf{ratio}(\mathsf{G}_{f,n,\varepsilon,m})$ as follows. For $i \in (n-1)$, $t \in \mathbb{Z}$ and $\mathcal{S} \subseteq \mathbb{Z}$ and $a \in \mathrm{Supp}(A_{i+1})$, let $\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(t,k) = \frac{\Pr[A_{i+1}=a|Y_{i+1}=t]}{\Pr[A_{i+1}=a|Y_i=k, X_{i+1}\in\mathcal{S}]}$.*

Lemma 4.14. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds. Let $\mathsf{G}_{f,n,\varepsilon,m}$, $\{X_i\}_{i\in(n)}$, $\{Y_i\}_{i\in(n)}$ and $\{A_i\}_{i\in(n)}$ be according to Definition 4.1, let $\{\mathcal{U}_{n,i,\varepsilon}\}_{i\in(n)}$ be according to Definition 4.9, let $\{\mathcal{X}_i\}_{i\in(n-1)}$ be according to Definition 4.11, and let $\mathsf{ratio} = \mathsf{ratio}(\mathsf{G}_{f,n,\varepsilon,m})$ be according to Definition 4.13.* [**Eliad's Note: Change in every place in the paper $c > 0$**] *Assume $|\varepsilon| \leq 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}$ and assume there exist $c > 1$, and set ensembles $\{\mathcal{A}_{i,k}\}_{i\in(n-1),k\in\mathbb{Z}}$, such that the following holds for every $i \in \mathbb{N}$ with $i \leq n - \log^{1.5} n$, and for every $k \in \mathcal{U}_{n,i,\varepsilon}$.*

1. $\Pr[A_{i+1} \notin \mathcal{A}_{i,k} \mid Y_i = k] \leq \frac{1}{n^2}$,
2. $\left|1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k)\right| \leq c \cdot \frac{\log^{\frac{1}{2}} n}{\sqrt{\ell_n(i+1)}} \cdot \left(\frac{|x|}{\sqrt{\ell_n(i+1)}} + 1\right)$, *for every $a \in \mathcal{A}_{i,k}$.*

Then, $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon}) \leq \varphi(c) \cdot \frac{\log^2 n}{n}$.

We prove Lemma 4.14 in the next section.

4.2.1 Proving Lemma 4.14

In the following we fix $n \in \mathbb{N}$, $m \in \mathbb{N}$, $\varepsilon \in [-4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}, 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}]$, a game $\mathsf{G}_{f,n,\varepsilon}$ and random variables $\{X_i\}$, $\{Y_i\}$, $\{V_i\}$ according to Definition 4.1. Throughout, we assume that n is larger than some universal constant (Lemma 4.14 trivially holds for small n's). For $i \in \mathbb{N}$, let $\mathcal{U}_i = \mathcal{U}_{n,i,\varepsilon}$ be according to Definition 4.9 and let $\mathsf{ratio} = \mathsf{ratio}(\mathsf{G}_{f,n,\varepsilon,m})$ be according to Definition 4.13.

The following random variables are associated with a random run of the above game $\mathsf{G}_{f,n,\varepsilon}$. For $i \in (n)$, let E_i be the event that $Y_i \in \mathcal{U}_i$, let $L_i = E_1 \bigwedge E_2 \bigwedge \ldots \bigwedge E_i \bigwedge \neg E_{i+1}$, letting $E_{n+1} = \emptyset$, and let $p_i = \Pr[L_i]$. In words, E_i is the event that Y_i is not too large, and L_i is the event that i is the first index with Y_{i+1} large. Note that $\{L_j\}_{j\in(n)}$ are disjoint events and that $\Pr\left[\bigcup_{j\in(n)} L_j\right] = \sum_{j\in(n)} p_j = 1$.

Claim 4.15. *It holds that*

$$\left|V_{i|k,a} - V_{i|k}\right| \le \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{S}}_{i+1}}\left[\left|V_{i+1|k+x} - V_{i|k}\right| \cdot \left|1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)\right|\right] + \Pr[X_{i+1} \notin \mathcal{S}]$$

for any $i \in (n-1)$, $k \in \mathbb{Z}$, $a \in \mathcal{D}(f)$, and $\mathcal{S} \subseteq \mathbb{Z}$.

Proof. Let $p_{\mathcal{S}} = \Pr[X_{i+1} \in \mathcal{S} \mid Y_i = k] = \Pr[X_{i+1} \in \mathcal{S}]$ and $q_{\mathcal{S}} = \Pr[X_{i+1} \notin \mathcal{S} \mid Y_i = k] = \Pr[X_{i+1} \notin \mathcal{S}]$. Then,

$$\begin{aligned} V_{i|k} &= \Pr[Y_n > 0 \mid Y_i = k] \\ &= p_s \cdot \Pr[Y_n > 0 \mid Y_i = k, X_{i+1} \in \mathcal{S}] + q_s \cdot \Pr[Y_n > 0 \mid Y_i = k, X_{i+1} \notin \mathcal{S}] \\ &= p_s \cdot \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{S}}_{i+1}}[\Pr[Y_n > 0 \mid Y_{i+1} = k+x]] + q_s \cdot p, \end{aligned} \tag{14}$$

for $p = \Pr[Y_n > 0 \mid Y_i = k, X_{i+1} \notin \mathcal{S}]$. In addition,

$$\begin{aligned} V_{i|k,a} &= \Pr[Y_n > 0 \mid Y_i = k, A_{i+1} = a] \\ &= p_s \cdot \Pr[Y_n > 0 \mid Y_i = k, A_{i+1} = a, X_{i+1} \in \mathcal{S}] + q_s \cdot \Pr[Y_n > 0 \mid Y_i = k, A_{i+1} = a, X_{i+1} \notin \mathcal{S}] \\ &= p_s \cdot \frac{\Pr[Y_n > 0 \wedge A_{i+1} = a \mid Y_i = k, X_{i+1} \in \mathcal{S}]}{\Pr[A_{i+1} = a \mid Y_i = k, X_{i+1} \in \mathcal{S}]} + q_s \cdot p' \\ &= p_s \cdot \frac{\mathrm{E}_{x\leftarrow X^{\mathcal{S}}_{i+1}}[\Pr[Y_n > 0 \wedge A_{i+1} = a \mid Y_i = k+x]]}{\Pr[A_{i+1} = a \mid Y_i = k, X_{i+1} \in \mathcal{S}]} + q_s \cdot p' \\ &= p_s \cdot \frac{\mathrm{E}_{x\leftarrow X^{\mathcal{S}}_{i+1}}[\Pr[Y_n > 0 \mid Y_i = k+x] \cdot \Pr[A_{i+1} = a \mid Y_i = k+x]]}{\Pr[A_{i+1} = a \mid Y_i = k, X_{i+1} \in \mathcal{S}]} + q_s \cdot p' \\ &= p_s \cdot \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{S}}_{i+1}}\left[V_{i+1|k+x} \cdot \frac{\Pr[A_{i+1} = a \mid Y_i = k+x]}{\Pr[A_{i+1} = a \mid Y_i = k, X_{i+1} \in \mathcal{S}]}\right] + q_s \cdot p' \\ &= p_s \cdot \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{S}}_{i+1}}\left[V_{i+1|k+x} \cdot \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)\right] + q_s \cdot p', \end{aligned} \tag{15}$$

for $p' = \Pr[Y_n > 0 \mid Y_i = k, A_{i+1} = a, X_{i+1} \notin \mathcal{S}]$. We conclude that

$$
\begin{aligned}
&\left|V_{i|k} - V_{i|k,a}\right| \\
&\leq p_s \cdot \left| \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[V_{i+1|k+x} \cdot (1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)) \right] \right| + q_s \cdot |p - p'| \\
&\leq \left| \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[(V_{i|k} + V_{i+1|k+x} - V_{i|k}) \cdot (1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)) \right] \right| + q_s \\
&\leq \left| \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[V_{i|k} \cdot (1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)) \right] \right| + \left| \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[(V_{i+1|k+x} - V_{i|k}) \cdot (1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)) \right] \right| + q_s \\
&\leq \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[\left|V_{i+1|k+x} - V_{i|k}\right| \cdot \left| 1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k) \right| \right] + q_s \\
&= \mathop{\mathrm{E}}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[\left|V_{i+1|k+x} - V_{i|k}\right| \cdot \left| 1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k) \right| \right] + \Pr[X_{i+1} \notin \mathcal{S}],
\end{aligned}
$$

where the fourth inequality holds since $\mathrm{E}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k) \right] = 1$, and therefore $\mathrm{E}_{x \leftarrow X^{\mathcal{S}}_{i+1}} \left[V_{i|k} \cdot (1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{S}}(k+x,k)) \right] = 0$. □

Claim 4.16. $\left|V_{i+1|k+x} - V_{i|k}\right| \leq \frac{2}{\sqrt{\ell_n(i+1)}}(\frac{|x|}{\sqrt{\ell_n(i+1)}} + 1)$, *for any* $i \in (n-1)$ *and* $k, x \in \mathbb{Z}$ *with* $|k|, |x| \leq \log n \cdot \sqrt{\mathsf{sum}_n(i+1) \cdot \log(n)}$.

Proof.

$$
\begin{aligned}
\left|V_{i+1|k+x} - V_{i|k}\right| &= \left| \mathop{\mathrm{E}}_{x' \leftarrow X_{i+1}} \left[V_{i+1|k+x} - V_{i+1|k+x'} \right] \right| \\
&= \left| \mathop{\mathrm{E}}_{x' \leftarrow X_{i+1}} \left[\widehat{\mathsf{B}}_{\mathsf{sum}_n(i+1),\varepsilon}(-k-x) - \widehat{\mathsf{B}}_{\mathsf{sum}_n(i+1),\varepsilon}(-k-x') \right] \right| \\
&\leq \mathop{\mathrm{E}}_{x' \leftarrow X_{i+1}} \left[\frac{|x - x'|}{\sqrt{\mathsf{sum}_n(i+1)}} \right] \\
&\leq \mathop{\mathrm{E}}_{x' \leftarrow X_{i+1}} \left[\frac{|x| + |x'|}{\sqrt{\mathsf{sum}_n(i+1)}} \right] \\
&= \frac{|x| + \mathrm{E}_{x' \leftarrow X_{i+1}} \left[|x'| \right]}{\sqrt{\mathsf{sum}_n(i+1)}} \\
&\leq \frac{|x| + \sqrt{2 \cdot \ell_n(i+1)}}{\sqrt{\mathsf{sum}_n(i+1)}} \\
&= \frac{|x| + \sqrt{2 \cdot \ell_n(i+1)}}{\sqrt{\frac{1}{2}\ell_n(i+1)(\ell_n(i+1)+1)}} \\
&\leq \sqrt{\frac{2}{\ell_n(i+1)}} \cdot \frac{|x|}{\sqrt{\ell_n(i+1)}} + \frac{2}{\sqrt{\ell_n(i+1)}} \\
&\leq \frac{2}{\sqrt{\ell_n(i+1)}}(\frac{|x|}{\sqrt{\ell_n(i+1)}} + 1),
\end{aligned}
$$

where the first inequality follows by Proposition 2.16, and the third one by Fact 2.13. □

Claim 4.17. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ (independent of the game) such that the following holds. Let $\{\mathcal{X}_i\}_{i\in(n-1)}$ be according to Definition 4.11, and let $k \in \mathbb{Z}$, $\lambda \geq 0$, $a \in \mathcal{D}(f)$, and $c > 1$ such that for every $x \in \mathcal{X}_i$,*

$$\left|1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k)\right| \leq c \cdot \frac{\log^\lambda n}{\sqrt{\ell_n(i+1)}} \cdot \left(\frac{|x|}{\sqrt{\ell_n(n+i)}} + 1\right). \tag{16}$$

Then, $\left|V_{i|k,a} - V_{i|k}\right| \leq \varphi(c) \cdot \frac{\log^\lambda n}{\ell_n(i)}$.

Proof.

$$\begin{aligned}
\left|V_{i|k,a} - V_{i|k}\right| &\leq \Pr[X_{i+1} \notin \mathcal{X}_i] + \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\left|V_{i+1|k+x} - V_{i|k}\right| \cdot \left|1 - \mathsf{ratio}^{\mathcal{X}_i}_{i,a}(k+x,k)\right|\right] \\
&\leq \frac{1}{\ell_n(i+1)} + \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\frac{2}{\sqrt{\ell_n(i+1)}}\left(\frac{|x|}{\sqrt{\ell_n(i+1)}} + 1\right) \cdot c \cdot \frac{\log^\lambda n}{\sqrt{\ell_n(i+1)}} \cdot \left(\frac{|x|}{\sqrt{\ell_n(i+1)}} + 1\right)\right] \\
&= \frac{1}{\ell_n(i+1)} + \frac{2c \cdot \log^\lambda n}{\ell_n(i+1)} \cdot \mathop{\mathrm{E}}_{x\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\frac{x^2}{\ell_n(i+1)} + 2 \cdot \frac{|x|}{\sqrt{\ell_n(i+1)}} + 1\right] \\
&\leq \frac{1}{\ell_n(i+1)} + \frac{2c \cdot \log^\lambda n}{\ell_n(i+1)} \cdot \left(\frac{2 \cdot \ell_n(i+1)}{\ell_n(i+1)} + 2 \cdot \frac{\sqrt{2 \cdot \ell_n(i+1)}}{\sqrt{\ell_n(i+1)}} + 1\right) \\
&= \frac{1 + 2 \cdot (2\sqrt{2}+3) \cdot c \cdot \log^\lambda n}{\ell_n(i+1)} \\
&\leq \frac{12 \cdot c \cdot \log^\lambda n}{\ell_n(i)},
\end{aligned}$$

where the first inequality holds by Claim 4.15, the second one holds by Claim 4.16, Equation (16) and Item 1 of Proposition 4.12, and the third one holds by Fact 2.13 using Items 2 and 3 of Proposition 4.12. □

Claim 4.18. *For any integer $i \in [\frac{n}{2}, n]$, it holds that $\Pr[E_i] \leq \frac{8\ell_n(i)\sqrt{\log n}}{n}$.*

Proof. Note that Y_i is the outcome of $\mathsf{sum}_n(1) - \mathsf{sum}_n(i+1)$ coins. Compute

$$\begin{aligned}
\mathsf{sum}_n(1) - \mathsf{sum}_n(i+1) &= \frac{1}{2}\left(\ell_n(1)(\ell_n(1)+1) - \ell_n(i+1)(\ell_n(i+1)+1)\right) \\
&= \frac{1}{2}\left(n(n+1) - (n-i)(n-i+1)\right) \\
&\geq \frac{1}{2}\left(n(n+1) - \frac{n}{2}\left(\frac{n}{2}+1\right)\right) \\
&\geq \frac{n^3}{4}.
\end{aligned} \tag{17}$$

By Proposition 2.14, the probability that Y_i equals a given value, is at most $\frac{1}{\sqrt{(\mathsf{sum}_n(1)-\mathsf{sum}_n(i+1))}} \leq \frac{2}{n}$ (recall we assume n is larger than a universal constant). Therefore,

$$\begin{aligned}
\Pr[E_i] &\leq 2\sqrt{8\mathsf{sum}_n(i+1)\log n}\cdot\frac{2}{n} \\
&= \frac{4\sqrt{8\cdot\mathsf{sum}_n(i+1)\log n}}{n} \\
&= \frac{4\sqrt{8\cdot\frac{1}{2}\cdot\ell_n(i+1)(\ell_n(i+1)+1)\log n}}{n} \\
&\leq \frac{4\sqrt{4\cdot\ell_n(i)^2\log n}}{n} \\
&= \frac{8\ell_n(i)\sqrt{\log n}}{n}.
\end{aligned}$$

□

Claim 4.19. *For any integer $i \in [\frac{n}{2}, n]$, it holds that $\sum_{j=i}^{n} p_j \leq \frac{8\ell_n(i)\sqrt{\log n}}{n}$.*

Proof. Since $\{L_j\}_{j=0}^{n}$ are disjoint and $\bigcup_{j=i}^{n} L_j \subseteq E_i$, it holds that $\sum_{j=i}^{n} p_j = \Pr[\bigcup_{j=i}^{n} L_i] \leq \Pr[E_i] \leq \frac{8\ell_n(i)\sqrt{\log n}}{n}$. □

Putting it together. We are finally ready to prove Lemma 4.14.

Proof Lemma 4.14. Let B be some strategy and let B' be a strategy that operates just like B, but does not abort (i.e., does not output 1), in round i (even if B does) in case $i \geq n - \log^{1.5} n$, or $i \geq i'$, where i' is the minimal index with $\overline{E_i}$. Proposition 4.8 and Claim 4.18 [**Eliad's Note: Explain why Proposition 4.8**] yield that

$$|\mathsf{val}_{\mathsf{B}}(\mathsf{G}_{f,n,\varepsilon}) - \mathsf{val}_{\mathsf{B}'}(\mathsf{G}_{f,n,\varepsilon})| \leq \frac{1}{n} + \frac{8\log^2 n}{n} \tag{18}$$

Let B'' be a strategy that operates just like B', but does not abort (even if B' does) in rounds $\{i,\ldots,n\}$, where i is the minimal index with $A_{i+1} \notin \mathcal{A}_{i,Y_i}$, and let $I'' = I(\mathsf{G}_{f,n,\varepsilon}, \mathsf{B}'')$ be according to Definition 4.2. By assumption 1, it holds that

$$|\mathsf{val}_{\mathsf{B}'}(\mathsf{G}_{f,n,\varepsilon}) - \mathsf{val}_{\mathsf{B}''}(\mathsf{G}_{f,n,\varepsilon})| \leq \Pr\left[\exists i \in (n-1)\colon Y_i \in \mathcal{U}_i \wedge A_{i+1} \notin \mathcal{A}_{i,Y_i}\right] \leq \frac{1}{n} \tag{19}$$

Consider a random run of $\mathsf{G}_{f,n,\varepsilon}$, and let J be the index with $L_J = 1$, letting $J = n$ in case no such index. The definition of B'' yields that $I'' \leq J$. Let $k = Y_{I''} \in \mathcal{U}_{I''}$ and let $a = A_{I''+1} \in \mathcal{A}_{I'',k}$.

By the definition of B'' and assumption 2, we can apply *Claim* 4.17 to deduce that

$$\left|V_{I''|k,a} - V_{I''|k}\right| \leq \frac{\varphi'(c)\cdot\log^{\frac{1}{2}} n}{\ell_n(I'')} \leq \frac{\varphi'(c)\cdot\log^{\frac{1}{2}} n}{\ell_n(J)} \tag{20}$$

where φ' is the function of *Claim* 4.17. It follows that [**Eliad's Note: Replace $\frac{1}{2}$ with 0.5 or something better**]

$$\begin{aligned}
\mathsf{val}_{\mathsf{B}''}(\mathsf{G}_{f,n,\varepsilon}) &\leq \sum_{i=0}^{n} \Pr\left[L_i\right] \cdot \frac{\varphi'(c) \cdot \log^{\frac{1}{2}} n}{\ell_n(i)} \\
&= \sum_{i=0}^{n} p_i \cdot \frac{\varphi'(c) \cdot \log^{\frac{1}{2}} n}{\ell_n(i)} \\
&\leq \varphi'(c) \cdot \log^{\frac{1}{2}} n \Big(\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \frac{p_i}{\ell_n(i)} + \sum_{i=\lceil \frac{n}{2} \rceil}^{n} \frac{p_i}{\ell_n(i)} \Big) \\
&\leq \varphi'(c) \cdot \log^{\frac{1}{2}} n \Big(\frac{1}{\ell_n(\lceil \frac{n}{2} \rceil - 1)} + \frac{8\sqrt{\log n}}{n} \cdot \sum_{i=\lceil \frac{n}{2} \rceil}^{n} \frac{1}{\ell_n(i)} \Big) \\
&\leq \varphi'(c) \cdot \log^{\frac{1}{2}} n \Big(\frac{1}{\frac{1}{2} \cdot \frac{n}{2}} + \frac{8\sqrt{\log n}}{n} \cdot \sum_{i=\lceil \frac{n}{2} \rceil}^{n} \frac{1}{n - i + 1} \Big) \\
&\leq \varphi'(c) \cdot \log^{\frac{1}{2}} n \Big(\frac{4}{n} + \frac{8 \log^{1.5} n}{n} \Big) \\
&\leq 9\varphi'(c) \cdot \frac{\log^2 n}{n},
\end{aligned} \tag{21}$$

where the third inequality holds by Claim 4.19 and Proposition 2.11, and the fifth one holds since $\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor + 1} \frac{1}{i} \leq \log n$. We conclude that $\mathsf{val}(\mathsf{G}_{f,n,\varepsilon}) \leq 9\varphi'(c) \cdot \frac{\log^2 n}{n} + \frac{2}{n} + \frac{8 \log^2 n}{n} \leq (9\varphi'(c) + 9) \frac{\log^2 n}{n}$. □

4.3 The Simple Game

Proof of Lemma 4.4. Recall that in the simple game, $f(i,k)$ draws a random sample from $\mathcal{B}er(V_{i|k})$, where $V_{i|k} = \widehat{\mathsf{B}}_{\mathsf{sum}_n(i+1),\varepsilon}(-k)$. We view the function f as the composition $g \circ h$, where $h(i,k)$ outputs $k + t$, for $t \leftarrow \mathcal{B}_{\mathsf{sum}_n(i+1),\varepsilon}$, and $g(k+t)$ outputs 1 if $k + t > 0$, and zero otherwise. Using Proposition 4.7, for bounding the value of $\mathsf{G}_{h,n,\varepsilon}$ it suffices to bound that of $\mathsf{G}_{h,n,\varepsilon}$.

We would like to assume that $|\varepsilon| \leq 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}$. Indeed, if this is not the case, then $\mathsf{G}_{h,n,\varepsilon} \notin (\frac{1}{n^2}, 1 - \frac{1}{n^2})$, and the proof follows by Proposition 4.8. Therefore, in the following we assume that $|\varepsilon| \leq 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}$.

In the following we fix $i \in (n - \log^{1.5} n)$, $x \in \mathcal{X}_i$ and $k \in \mathcal{U}_{n,i,\varepsilon}$, where $\mathcal{X}_i$ is according to Definition 4.11 and $\mathcal{U}_{n,i,\varepsilon}$ is according to Definition 4.9. Let

$$\mathcal{A}_{i,k} = \{a \in \mathbb{Z} \colon |a - k| \leq d\sqrt{\log n \cdot \mathsf{sum}_n(i+1)}\} \tag{22}$$

where $d = 8$. Since $A_{i+1} - k$ is distributed according to $\mathcal{B}_{\mathsf{sum}_n(i+1),\varepsilon}$, and since $|\varepsilon \cdot \mathsf{sum}_n(i+1)| \leq 4\sqrt{\log n \cdot \mathsf{sum}_n(i+1)}$, it holds by Hoeffding's inequality (Fact 2.12) that

$$\Pr\left[A_{i+1} \notin \mathcal{A}_{i,k}\right] \leq \frac{1}{n^2} \tag{23}$$

In the following we fix $a = k + t \in \mathcal{A}_{i,k}$, and let $t_0 = t - \varepsilon \cdot \mathsf{sum}_n(i+1)$. Note that $|t_0| = |t - \varepsilon \cdot \mathsf{sum}_n(i+1)| = |a - k - \varepsilon \cdot \mathsf{sum}_n(i+1)| \leq |a| + |k + \varepsilon \cdot \mathsf{sum}_n(i+1)| \leq (d+8)\sqrt{\mathsf{sum}_n(i+1)\log n}$. Compute

$$\begin{aligned}
\frac{1}{\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k)} &= \frac{\Pr[A_{i+1} = k+t \mid Y_i = k, X_{i+1} \in \mathcal{X}_i]}{\Pr[A_{i+1} = k+t \mid Y_{i+1} = k+x]} \\
&= \mathop{\mathrm{E}}_{x' \leftarrow X^{\mathcal{X}_i}_{i+1}} \left[\frac{\mathcal{B}_{\mathsf{sum}_n(i+1),\varepsilon}(t - x')}{\mathcal{B}_{\mathsf{sum}_n(i+1),\varepsilon}(t - x)} \right] \\
&\in \mathop{\mathrm{E}}_{x' \leftarrow X^{\mathcal{X}_i}_{i+1}} \left[\exp\left(\frac{-2 \cdot t_0 \cdot x + x^2 + 2 \cdot t_0 \cdot x' - x'^2}{2 \cdot \mathsf{sum}_n(i+1)} \right) \cdot \left(1 \pm \varphi_1(d) \frac{\log^{1.5}(\mathsf{sum}_n(i+1))}{\sqrt{\mathsf{sum}_n(i+1)}} \right) \right] \\
&\subseteq \left(1 \pm \varphi_2(d) \left(\sqrt{\frac{\log n}{\ell_n(i)}} (1 + \frac{|x|}{\sqrt{\ell_n(i)}}) \right) \right) \cdot \left(1 \pm \varphi_1(d) (\frac{\log^{1.5}(\mathsf{sum}_n(i+1))}{\sqrt{\mathsf{sum}_n(i+1)}} \right) \\
&\subseteq 1 \pm \varphi_3(d) \left(\sqrt{\frac{\log n}{\ell_n(i)}} \left(1 + \frac{|x|}{\sqrt{\ell_n(i)}} \right) \right),
\end{aligned} \tag{24}$$

for some functions $\varphi_1, \varphi_2, \varphi_3 \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ (independent of the game). The first belonging holds by Proposition 2.15, and the first containment by Proposition 2.19. Recalling that $i \leq n - \log^{1.5} n$, it follows that

$$\varphi_3(d) \cdot \sqrt{\frac{\log n}{\ell_n(i+1)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_n(i+1)}}) \in O\left(\sqrt{\frac{\log n}{\ell_n(i+1)}} \cdot \log(\ell_n(i+1)) \right) \in o(1) \tag{25}$$

Therefore,

$$\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k) \in 1 \pm 2\varphi_3(d) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_n(i)}}) \tag{26}$$

and thus

$$\left| 1 - \mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k) \right| \leq 2\varphi_3(d) \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \cdot (1 + \frac{|x|}{\sqrt{\ell_n(i)}}) \tag{27}$$

Since the above holds for every $i \in (n - \log^{1.5} n)$, $k \in \mathcal{U}_{n,i,\varepsilon}$, $a \in \mathcal{A}_{i,k}$ and $x \in \mathcal{X}_i$, and recalling Equation (23), we can apply Lemma 4.14, to get that $\mathsf{val}(\mathsf{G}_{h,n,\varepsilon}) \leq \xi \cdot \frac{\log^2 n}{n}$, for some universal constant (independent of the game) $\xi \geq 0$. □

4.4 The Hypergeometric Game

Proof of Lemma 4.5. Recall that In the hypergeometric game, the output of $f(i,k)$ is defined be the following process: a random subset $\mathcal{S}'$ of size $\mathsf{sum}_n(i+1)$ is drawn uniformly at random from a $2\mathsf{sum}_n(1)$-size set $\mathcal{S}$ over $\{-1,1\}$ with $w(\mathcal{S}) = p$, and then the output is set to one, if $k + w(\mathcal{S}') \geq 0$, where $w(\mathcal{S}') = \sum_{s \in \mathcal{S}'} s$. Recall that $p \in \mathbb{Z}$ with $|p| \leq \gamma \cdot \sqrt{\log n \cdot \mathsf{sum}_n(1)}$, is a parameter of the game.

We view the function f as $g \circ h$. Where $h(i,k)$ is defined by the following process: a random subset $\mathcal{S}_i$ of size $2\mathsf{sum}_n(i+1)$ is drawn uniformly at random from a $2\mathsf{sum}_n(1)$-size set $\mathcal{S}$ over $\{-1,1\}$ with $w(\mathcal{S}) = p$, and outputs $(w(\mathcal{S}_i), k+t)$ for $t \leftarrow \mathcal{HG}_{2\mathsf{sum}_n(i+1),w(\mathcal{S}_i),\mathsf{sum}_n(i+1)}$. And $g(p',k')$ outputs one if $k' \geq 0$, and zero otherwise. Since $\Pr[g \circ h(i,k) = 1] = \Pr[f(i,k) = 1]$, by Proposition 4.7 it suffices to bound the value of the game $\mathsf{G}_{h,n,\varepsilon}$.

As in the proof of Lemma 4.4, we can assume without loss of generality that $|\varepsilon| \leq 4\sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}$. In the following we fix $i \in (n - \log^{1.5} n)$, $x \in \mathcal{X}_i$ and $k \in \mathcal{U}_{n,i,\varepsilon}$, where $\mathcal{X}_i$ is according to Definition 4.11 and $\mathcal{U}_{n,i,\varepsilon}$ is according to Definition 4.9. Let

$$\mathcal{A}_{i,k} = \{(p',k') \in \mathbb{Z}^2 \colon |p'|, |k'-k| \leq d(\gamma)\sqrt{\log(n) \cdot \mathsf{sum}_n(i+1)}\}, \tag{28}$$

where $d(\gamma) = \gamma + 8$. Since $A_{i+1} = (p', k+t)$ for $p' \leftarrow \mathcal{HG}_{2\mathsf{sum}_n(1),p,2\mathsf{sum}_n(i+1)}$ and $t \leftarrow \mathcal{HG}_{2\mathsf{sum}_n(i+1),p',\mathsf{sum}_n(i+1)}$, by Hoeffding's inequality for hypergeometric distribution (Fact 2.20) it holds that

$$\Pr[A_{i+1} \notin \mathcal{A}_{i,k}] \leq \frac{1}{n^2} \tag{29}$$

In the following we fix $a = (p', k+t) \in \mathcal{A}_{i,k}$. Compute

$$\begin{aligned}
\frac{1}{\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k)} &= \frac{\Pr[A_{i+1} = (p',k+t) \mid Y_i = k, X_{i+1} \in \mathcal{X}_i]}{\Pr[A_{i+1} = (p',k+t) \mid Y_{i+1} = k+x]} \\
&= \mathop{\mathrm{E}}_{x' \leftarrow X^{\mathcal{X}_i}_{i+1}} \left[\frac{\mathcal{HG}_{2\mathsf{sum}_n(i+1),p',\mathsf{sum}_n(i+1)}(t-x')}{\mathcal{HG}_{2\mathsf{sum}_n(i+1),p',\mathsf{sum}_n(i+1)}(t-x)}\right] \\
&\in \mathop{\mathrm{E}}_{x' \leftarrow X^{\mathcal{X}_i}_{i+1}} \left[\exp\left(\frac{-2(t-p')x + x^2 + 2(t-p')x' - x'^2}{\mathsf{sum}_n(i+1)}\right)\right] \cdot \left(1 \pm \varphi_1(\gamma) \cdot \frac{\log^{1.5} \mathsf{sum}_n(i+1)}{\sqrt{\mathsf{sum}_n(i+1)}}\right) \\
&\subseteq \left(1 \pm \varphi_2(\gamma)\sqrt{\frac{\log n}{\ell_n(i)}}\left(1 + \frac{|x|}{\sqrt{\ell_n(i)}}\right)\right) \cdot \left(1 \pm \varphi_1(\gamma) \cdot \frac{\log^{1.5}(\mathsf{sum}_n(i+1))}{\sqrt{\mathsf{sum}_n(i+1)}}\right) \\
&\subseteq 1 \pm \varphi_3(\gamma)\sqrt{\frac{\log n}{\ell_n(i)}}\left(1 + \frac{|x|}{\sqrt{\ell_n(i)}}\right),
\end{aligned} \tag{30}$$

for some functions $\varphi_1, \varphi_2, \varphi_3 \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ (independent of the game). The first belonging holds by Proposition 2.21, and the first containment by Proposition 2.19.[**Iftach's Note: give details after deadline**] Recalling that $i \leq n - \log^{1.5} n$, it follows that (see the proof of Lemma 4.4)

$$\varphi_3(\gamma) \cdot \sqrt{\frac{\log n}{\ell_n(i+1)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_n(i+1)}}\right) \in o(1) \tag{31}$$

Therefore,

$$\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k) \in 1 \pm 2\varphi_3(\gamma)\sqrt{\frac{\log n}{\ell_n(i)}} \cdot \left(1 + \frac{|x|}{\sqrt{\ell_n(i)}}\right) \tag{32}$$

and thus

$$\left|1-\mathsf{ratio}^{\mathsf{G}}_{i,a,\mathcal{X}_i}(k+x,k)\right| \leq 2\varphi_3(\gamma)\sqrt{\frac{\log n}{\ell_n(i)}}\cdot\left(1+\frac{|x|}{\sqrt{\ell_n(i)}}\right) \tag{33}$$

Since the above holds for every $i \in (n-\log^{1.5} n)$, $k \in \mathcal{U}_{n,i,\varepsilon}$, $a \in \mathcal{A}_{i,k}$ and $x \in \mathcal{X}_i$, and recalling Equation (29), we can apply Lemma 4.14 to get that $\mathsf{val}(\mathsf{G}_{h,n,\varepsilon}) \leq \varphi(\gamma)\cdot\frac{\log^2 n}{n}$, for some universal function $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ (independent of the game). □

4.5 The Vector Game

Proof of Lemma 4.6. Recall that in the vector game, for $i \in [n]$ and $k \in \mathbb{Z}$, the output of $f(i,k)$ is a vector in $v \in \{-1,1\}^{q=9\cdot\mathsf{sum}_n(1)}$, where every coordinate of v is, independently, drawn from [**Eliad's Note: Decide on the definition of Ber!!!**] $\mathcal{B}er(\varepsilon_{i,k})$ for

$$\varepsilon_{i,k} := \mathcal{B}^{-1}(\mathsf{sum}_n(i+1), 0, -k, \mathsf{sum}_n(1)) \tag{34}$$

In the following we fix $i \in (n-\log^{1.5} n)$, $x \in \mathcal{X}_i$ and $k \in \mathcal{U}_{n,i,0}$, where $\mathcal{X}_i$ is according to Definition 4.11 and $\mathcal{U}_{n,i,0}$ is according to Definition 4.9, and let $s_i = \mathsf{sum}_n(i+1)\cdot\mathsf{sum}_n(1)$.

Note that

$$\Pr\left[f(i,k)=v\right] = 2^{-n}\cdot(1+\varepsilon_{i,k})^{\frac{q}{2}+\frac{w(v)}{2}}\cdot(1-\varepsilon_{i,k})^{\frac{q}{2}-\frac{w(v)}{2}} \tag{35}$$

for every $v \in \{-1,1\}^q$, where $w(v) = \sum_{j\in[q]} v_j$. Let

$$\mathcal{A}_{i,k} = \{v \in \{-1,1\}^q\colon\ |w(v)| \leq \sqrt{d\cdot\log n\cdot q}\} \tag{36}$$

where d is a universal constant (independent of the game) to be determined by the analysis. Proposition 2.17 yields that $\varepsilon_{i,k} \in \frac{k}{\sqrt{s_i}} \pm \frac{\log^2(\mathsf{sum}_n(i+1))}{\sqrt{s_i}}$. Recall that $k \in \mathcal{U}_{n,i,0}$, it follows that $|k| \leq \sqrt{8\log n\cdot\mathsf{sum}_n(i+1)}$. Therefore, $\left|\frac{k}{\sqrt{s_i}}\right| \leq \frac{\sqrt{8\log n\cdot\mathsf{sum}_n(i+1)}}{\sqrt{\mathsf{sum}_n(i+1)\cdot\mathsf{sum}_n(1)}} = \sqrt{\frac{72\cdot\log n}{q}}$, and thus, $|\varepsilon_{i,k}| \leq 9\cdot\sqrt{\frac{\log n}{q}}$. Hence, by Hoeffding's bound (Fact 2.12), setting $d = 144$ yields that

$$\begin{aligned}\Pr\left[A_{i+1}\notin\mathcal{A}_{i,k}\right] &= \Pr_{z\leftarrow\mathcal{B}_{q,\varepsilon_{i,k}}}\left[|z| > \sqrt{d\cdot\log n\cdot q}\right]\\ &\leq \Pr_{z\leftarrow\mathcal{B}_{q,\varepsilon_{i,k}}}\left[\left|z-9\sqrt{\log n\cdot q}\right| > 3\sqrt{\log n\cdot q}\right]\\ &\leq \frac{1}{n^2}\end{aligned} \tag{37}$$

In the following we fix $v \in \mathcal{A}_{i,k}$. Compute

$$\begin{aligned}\Pr[A_{i+1}=v \mid Y_{i+1}=k+x] &= 2^{-q}\cdot(1+\varepsilon_{i,k+x})^{\frac{q}{2}+w(v)}(1-\varepsilon_{i,k+x})^{\frac{q}{2}-\frac{w(v)}{2}}\\ &= 2^{-q}\cdot(1-\varepsilon^2_{i,k+x})^{\frac{q}{2}-\frac{w(v)}{2}}(1+\varepsilon_{i,k+x})^{w(v)}\end{aligned} \tag{38}$$

Since $1+z \le e^z$ for $z \in \mathbb{R}$, it holds that

$$\Pr[A_{i+1}=v \mid Y_{i+1}=k+x] \le 2^{-q} \cdot \exp\left(-\varepsilon_{i,k+x}^2(\frac{q}{2}-\frac{w(v)}{2})+\varepsilon_{i,k+x}\cdot w(v)\right) \tag{39}$$

Recalling that $k \in \mathcal{U}_{n,i,0}$, Proposition 2.17 yields that $\varepsilon_{i,k+x} \in (-\frac{1}{2},\frac{1}{2})$. Using the inequality $1+z \ge e^{z-z^2}$ for $z \in (-\frac{1}{2},\frac{1}{2})$, we deduce that

$$\begin{aligned}\Pr[A_{i+1}=v \mid Y_{i+1}=k+x] &\ge 2^{-q}\cdot e^{(-\varepsilon_{i,k+x}^2-\varepsilon_{i,k+x}^4)(\frac{q}{2}-\frac{w(v)}{2})}\cdot e^{(\varepsilon_{i,k+x}-\varepsilon_{i,k+x}^2)\cdot w(v)} \\ &= 2^{-q}\cdot e^{-\varepsilon_{i,k+x}^2(\frac{q}{2}-\frac{w(v)}{2})}\cdot e^{\varepsilon_{i,k+x}\cdot w(v)}\cdot e^{-\varepsilon_{i,k+x}^4(\frac{q}{2}-\frac{w(v)}{2})-\varepsilon_{i,k+x}^2 w(v)} \\ &= 2^{-q}\cdot\exp\left(-\varepsilon_{i,k+x}^2(\frac{q}{2}-\frac{w(v)}{2})+\varepsilon_{i,k+x}\cdot w(v)\right)\cdot(1-\mathsf{error}(x))\end{aligned} \tag{40}$$

for

$$\mathsf{error}(x) := 1-\exp\left(-\varepsilon_{i,k+x}^4(\frac{q}{2}-\frac{w(v)}{2})-\varepsilon_{i,k+x}^2\cdot w(v)\right) \tag{41}$$

We can now write,

$$\Pr[A_{i+1}=v \mid Y_{i+1}=k+x] \in 2^{-q}\cdot\exp\left(-\varepsilon_{i,k+x}^2(\frac{q}{2}-\frac{w(v)}{2})+\varepsilon_{i,k+x}\cdot w(v)\right)(1\pm\mathsf{error}(x)) \tag{42}$$

Let $x' \in \mathcal{X}_i$, and assume, without loss of generality, that $|\mathsf{error}(x)| \ge |\mathsf{error}(x')|$. compute

$$\begin{aligned}&\frac{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x']}{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x]} \\ &\in \frac{\exp\left(-\varepsilon_{i,k+x'}^2(\frac{q}{2}-\frac{w(v)}{2})+\varepsilon_{i,k+x'}\cdot w(v)\right)}{\exp\left(-\varepsilon_{i,k+x}^2(\frac{q}{2}-\frac{w(v)}{2})+\varepsilon_{i,k+x}\cdot w(v)\right)}\cdot(1\pm 2\cdot\mathsf{error}(x)) \\ &= \exp\left((\varepsilon_{i,k+x}-\varepsilon_{i,k+x'})\left[(\varepsilon_{i,k+x}+\varepsilon_{i,k+x'})(\frac{q}{2}-\frac{w(v)}{2})-w(v)\right]\right)(1\pm 2\cdot\mathsf{error}(x)) \\ &\subseteq \exp\left((\frac{x-x'}{\sqrt{s_i}}\pm\frac{\log^2 n}{\sqrt{s_i}})\left[(\frac{2k+x+x'}{\sqrt{s_i}}\pm\frac{\log^2 n}{\sqrt{s_i}})\cdot(\frac{q}{2}-\frac{w(v)}{2})-w(v)\right]\right)\cdot(1\pm 2\cdot\mathsf{error}(x)) \\ &\subseteq \exp\left((\frac{x-x'}{\mathsf{sum}_n(i+1)}\pm\frac{\log^2 n}{\mathsf{sum}_n(i+1)})\left[(\frac{2k+x+x'}{\mathsf{sum}_n(1)}\pm\frac{\log^2 n}{\mathsf{sum}_n(1)})\cdot(\frac{q}{2}-\frac{w(v)}{2})\pm w(v)\right]\right)\cdot(1\pm 2\cdot\mathsf{error}(x)),\end{aligned} \tag{43}$$

and therefore,

$$\frac{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x']}{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x]} \in \exp\left((\frac{x-x'}{\mathsf{sum}_n(i+1)}\pm\frac{\log^2 n}{\mathsf{sum}_n(i+1)})\cdot\alpha\right)\cdot(1\pm 2\cdot\mathsf{error}(x))$$

for some $\alpha \in (\frac{2k+x+x'}{\mathsf{sum}_n(1)}\pm\frac{\log^2 n}{\mathsf{sum}_n(1)})\cdot(\frac{q}{2}-w(v))\pm w(v)$, where the first containment of the previous calculation holds by Proposition 2.17. By taking large enough universal constant $d'>0$, we can bound $|\alpha|$ and $|\mathsf{error}(x)|$ by

$$|\alpha| \le d'\cdot\sqrt{\log n\cdot\mathsf{sum}_n(i+1)} \tag{44}$$

and

$$
\begin{aligned}
|\mathsf{error}(x)| &= \left|1 - \exp\left(-\varepsilon_{i,k+x}^4 (\frac{q}{2} - \frac{w(v)}{2}) - \varepsilon_{i,k+x}^2 \cdot w(v)\right)\right| \\
&\in \left|1 - \exp\left(-\left(\frac{k+x}{\sqrt{s_i}} \pm \frac{\log^2(\mathsf{sum}_n(i+1))}{\sqrt{s_i}}\right)^4 (\frac{q}{2} - \frac{w(v)}{2}) - \left(\frac{k+x}{\sqrt{s_i}} \pm \frac{\log^2(\mathsf{sum}_n(i+1))}{\sqrt{s_i}}\right)^2 w(v)\right)\right| \\
&\leq 1 - \exp\left(-\left(3 \cdot \sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}\right)^4 \cdot 5 \cdot \mathsf{sum}_n(1) - \left(3 \cdot \sqrt{\frac{\log n}{\mathsf{sum}_n(1)}}\right)^2 \cdot \sqrt{9d \cdot \mathsf{sum}_n(1) \cdot \log n}\right) \\
&\leq 1 - (1 - \frac{d' \log^{1.5} n}{\sqrt{\mathsf{sum}_n(1)}}) \\
&= d' \frac{\log^{1.5} n}{\sqrt{\mathsf{sum}_n(1)}},
\end{aligned}
$$

where the first inequality means that the right expression is an upper bound on all the numbers in the set specified in the left expression. In addition, the first belonging holds by Proposition 2.17 and the second inequality holds by the bounds on k, x and $w(v)$. Since

$$
\begin{aligned}
&\exp\left(\frac{\log^2 n}{\mathsf{sum}_n(i+1)} \cdot \alpha\right) \qquad (45) \\
&\qquad \leq 1 + 2 \cdot \frac{\log^2 n}{\mathsf{sum}_n(i+1)} \cdot \alpha \\
&\qquad \leq 1 + 2 \cdot \frac{\log^2 n}{\mathsf{sum}_n(i+1)} \cdot d' \cdot \sqrt{\log n \cdot \mathsf{sum}_n(i+1)} \\
&\qquad \leq 1 + 2d' \cdot \frac{\log^{2.5} n}{\sqrt{\mathsf{sum}_n(i+1)}},
\end{aligned}
$$

it follows that

$$
\frac{\Pr[A_{i+1} = v \mid Y_{i+1} = k + x']}{\Pr[A_{i+1} = v \mid Y_{i+1} = k + x]} \in \exp\left(\frac{x - x'}{\mathsf{sum}_n(i+1)} \cdot \alpha\right) \cdot \left(1 \pm \frac{\log^3 n}{\sqrt{\mathsf{sum}_n(i+1)}}\right) \qquad (46)
$$

and thus

$$\begin{aligned}
\frac{1}{\mathsf{ratio}^{\mathsf{G}}_{i,v,\mathcal{X}_i}(k+x,k)} &= \frac{\Pr[A_{i+1}=v \mid Y_i=k, X_{i+1}\in\mathcal{X}_i]}{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x]} \\
&= \frac{\mathrm{E}_{x'\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\Pr[A_{i+1}=v \mid Y_i=k+x']\right.}{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x]} \\
&= \mathop{\mathrm{E}}_{x'\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\frac{\Pr[A_{i+1}=v \mid Y_i=k+x']}{\Pr[A_{i+1}=v \mid Y_{i+1}=k+x]}\right] \\
&\in \mathop{\mathrm{E}}_{x'\leftarrow X^{\mathcal{X}_i}_{i+1}}\left[\exp\left(\frac{\alpha x-\alpha x'}{\mathsf{sum}_n(i+1)}\right)\cdot\left(1\pm\frac{\log^3 n}{\mathsf{sum}_n(i+1)}\right)\right] \\
&\subseteq \left(1\pm\varphi_1(d)\cdot\sqrt{\frac{\log n}{\ell_n(i+1)}}\cdot(1+\frac{|x|}{\sqrt{\ell_n(i+1)}})\right)\cdot\left(1\pm\frac{\log^3 n}{\mathsf{sum}_n(i+1)}\right) \\
&\subseteq 1\pm\varphi_2(d)\sqrt{\frac{\log n}{\ell_n(i+1)}}\cdot(1+\frac{|x|}{\sqrt{\ell_n(i+1)}}).
\end{aligned} \tag{47}$$

for some functions $\varphi_1,\varphi_2\colon \mathbb{R}^+\mapsto\mathbb{R}^+$ (independent of the game). The first belonging follows by Equation (46), and the first containment by Proposition 2.19. Recalling that $i\le n-\log^{1.5} n$, it follows that (see the proof of Lemma 4.4)

$$\sqrt{\frac{\log n}{\ell_n(i+1)}}\cdot(1+\frac{|x|}{\sqrt{\ell_n(i+1)}})\in o(1) \tag{48}$$

Therefore,

$$\mathsf{ratio}^{\mathsf{G}}_{i,v,\mathcal{X}_i}(k+x,k)\in 1\pm 2\varphi_2(d)\cdot\sqrt{\frac{\log n}{\ell_n(i)}}\cdot(1+\frac{|x|}{\sqrt{\ell_n(i)}}) \tag{49}$$

and thus

$$\left|1-\mathsf{ratio}^{\mathsf{G}}_{i,v,\mathcal{X}_i}(k+x,k)\right|\le 2\varphi_2(d)\cdot\sqrt{\frac{\log n}{\ell_n(i)}}\cdot(1+\frac{|x|}{\sqrt{\ell_n(i)}}) \tag{50}$$

Since the above holds for every $i\in(n-\log^{1.5} n)$, $k\in\mathcal{U}_{n,i,\varepsilon}$, $v\in\mathcal{A}_{i,k}$ and $x\in\mathcal{X}_i$, and recalling Equation (37), we can apply Lemma 4.14 to get that $\mathsf{val}(\mathsf{G}_{h,n,\varepsilon})\le\xi\cdot\frac{\log^2 n}{n}$, for some universal constant $\xi\ge 0$. □

Acknowledgment

We are very grateful to Yuval Ishai, Yishay Mansour, Eran Omri and Alex Samorodnitsky for very useful discussions. We also thank Eran for encouraging us to tackle this beautiful problem.

References

[1] Abramowitz, M. and Stegun, I. A., editors. *Handbook of Mathematical Functions*. Dover Publications, 1964.

[2] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. C. Yao. Quantum bit escrow. In *STOC: ACM Symposium on Theory of Computing (STOC)*, 2000.

[3] W. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In *Advances in Cryptology – EUROCRYPT 2001*, 2001.

[4] N. Alon and M. Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM Journal on Computing*, pages 46–54, 1993.

[5] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004.

[6] A. Ambainis, H. Buhrman, Y. Dodis, and H. Röhrig. Multiparty quantum coin flipping. In *Proceedings of the 18th Annual IEEE Conference on Computational Complexity*, pages 250–259, 2004.

[7] A. Beimel, E. Omri, and I. Orlov. Protocols for multiparty coin toss with dishonest majority. In *Advances in Cryptology – CRYPTO 2010*, pages 538–557, 2010.

[8] A. Beimel, Y. Lindell, E. Omri, and I. Orlov. $1/p$-secure multiparty computation without honest majority and the best of both worlds. pages 277–296, 2011.

[9] M. Ben-Or and N. Linial. Collective coin flipping. *ADVCR: Advances in Computing Research*, 5, 1989.

[10] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, 1988.

[11] I. Berman, I. Haitner, and A. Tentes. Coin flipping of any constant bias implies one-way functions. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*.

[12] M. Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1983.

[13] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[14] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 2000.

[15] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 364–369, 1986.

[16] R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes. Manuscript, 1993.

[17] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. On the black-box complexity of optimally-fair coin tossing. In *tcc11*, pages 450–467, 2011.

[18] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[19] U. Feige. Noncryptographic selection protocols. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS)*, 1999.

[20] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC)*, pages 197–206, 2008.

[21] O. Goldreich. *Foundations of Cryptography – VOLUME 2: Basic Applications*. Cambridge University Press, 2004.

[22] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, pages 691–729, 1991. Preliminary version in *FOCS'86*.

[23] S. D. Gordon and J. Katz. Partial fairness in secure two-party computation. pages 157–176, 2010.

[24] S. D. Gordon, C. Hazay, J. Katz, and Y. Lindell. Complete fairness in secure two-party computation. pages 413–422, 2008.

[25] S. D. Gordon, C. Hazay, J. Katz, and Y. Lindell. Complete fairness in secure two-party computation. *Journal of the ACM*, 58(6):24, 2011.

[26] I. Haitner. Implementing oblivious transfer using collection of dense trapdoor permutations. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004*, pages 394–409, 2004.

[27] I. Haitner and E. Omri. Coin Flipping with Constant Bias Implies One-Way Functions. pages 110–119, 2011.

[28] I. Haitner, M. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, pages 1153–1218, 2009.

[29] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[30] Y. Kalai. Smooth projective hashing and two-message oblivious transfer. In *Advances in Cryptology – EUROCRYPT 2005*, 2005.

[31] J. Katz. On achieving the "best of both worlds" in secure multiparty computation. pages 11–20, 2007.

[32] Y. Lindell. Parallel coin-tossing and constant-round secure two-party computation. *Journal of Cryptology*, pages 143–184, 2003.

[33] H. K. Maji, M. Prabhakaran, and A. Sahai. On the Computational Complexity of Coin Flipping. In *Proceedings of the 51th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 613–622, 2010.

[34] T. Moran and M. Naor. Basing cryptographic protocols on tamper-evident seals. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 2005.

[35] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. In *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2009*, pages 1–18, 2009.

[36] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, pages 151–158, 1991.

[37] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *SODA*, pages 448–457, 2001.

[38] A. Russell and D. Zuckerman. Perfect information leader election in log* n + 0 (1) rounds. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS)*, 1999.

[39] M. Saks. A robust noncryptographic protocol for collective coin flipping. *SIJDM: SIAM Journal on Discrete Mathematics*, 2, 1989.

[40] M. Scala. Hypergeometric tail inequalities: ending the insanity, 2009.

A Missing Proofs

This section contains missing proofs for statement given in Sections 2.7 to 2.9.

A.1 Basic Inequalities

Proposition A.1 (Restatement of Proposition 2.11)**.** *Let $n \in \mathbb{N}$, $\alpha > 0$, $k \in [n]$ and let $\{p_j\}_{j=k}^{n}$ be a set of non-negative numbers such that $\sum_{j=i}^{n} p_j \leq \alpha \cdot (n+1-i)$ for every $i \in \{k, k+1, \ldots, n\}$. Then, $\sum_{j=k}^{n} \frac{p_j}{(n+1-j)} \leq \alpha \cdot \sum_{j=k}^{n} \frac{1}{(n+1-j)}$.*

[Eliad's Note: check the use in bounds.tex]

Proof. We prove the proposition by showing that for every set $\mathcal{S} = \{p_j\}_{j=k}^{n}$ satisfying the proposition's constrains, it holds that $\mathsf{val}(\mathcal{S}) := \sum_{j=k}^{n} \frac{p_j}{(n+1-i)} \leq \sum_{j=k}^{n} \frac{\alpha}{(n+1-i)}$. Let $\mathcal{S} = \{p_j\}_{j=k}^{n}$ be a set that satisfying the proposition's constrains with maximal $\mathsf{val}(\mathcal{S})$. Assume not all elements of $\mathcal{S}$ equal α, and let $i^* \in \{k, k+1, \ldots, n\}$ be the largest index such that $p_{i^*} \neq \alpha$. It follows that $\sum_{j=i^*}^{n} p_j \leq \alpha \cdot (n+1-i^*)$. Since $\sum_{j=i^*+1}^{n} p_j = \alpha \cdot (n-i^*)$, it follows that $p_{i^*} + \alpha(n-i^*) \leq \alpha \cdot (n+1-i^*)$, and thus $p_{i^*} \leq \alpha$. Since we assume $p_{i^*} \neq \alpha$, it follows that $p_{i^*} < \alpha$.

Assume $i^* = k$, then by changing p_{i^*} to α, and get a set $\mathcal{S}'$ with $\mathsf{val}(\mathcal{S}') > \mathsf{val}(\mathcal{S})$, in contraction to the maximality of $\mathcal{S}$.

Assume $i^* > k$ and let $\delta = \alpha - p_{i^*} > 0$. Let $\mathcal{S}' = \{p'_j\}_{j=k}^n$ defined by

$$p'_j = \begin{cases} p_j + \delta, & j = i^*, \\ p_j - \delta, & j = i^* - 1, \\ p_j, & \text{otherwise.} \end{cases}$$

Note that $\mathcal{S}'$ fulfills proposition's constrains, and

$$\mathsf{val}(\mathcal{S}') = \sum_{j=k}^{n} \frac{p'_j}{n-j+1} = \sum_{j=k}^{n} \frac{p_j}{n-j+1} + \frac{\delta}{n-i^*+1} - \frac{\delta}{n-i^*+2} > \sum_{j=k}^{n} \frac{p_j}{n-j+1} = \mathsf{val}(\mathcal{S}),$$

in contraction to the maximality of $\mathcal{S}$. □

A.2 Facts About the Binomial Distribution

We will make use of the following estimation for the binomial coefficient.

Proposition A.2. *For every $n \in \mathbb{N}$ and $t \in \mathbb{Z}$ such that $|t| \leq n^{\frac{3}{5}}$ and $\frac{n+t}{2} \in \mathbb{N}$, it holds that:*

$$\binom{n}{\frac{n+t}{2}} \cdot 2^{-n} \in (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}},$$

where $\mathsf{error} = \xi \cdot (\frac{|k|^3}{n^2} + \frac{1}{n})$ for some universal constant $\xi \geq 0$.

Proof. In the following we focus on $n \geq 200$, smaller n's are handled by setting the value of ξ to be large enough on these values. We also assume that n and t are even, the proof of the odd case is analogous. Let $m := \frac{n}{2} \geq 100$ and $k := \frac{t}{2}$. Stirling's formula states that for every $\ell \in \mathbb{N}$ it holds that $1 \leq \frac{\ell!}{\sqrt{2\pi\ell}\cdot(\frac{\ell}{e})^\ell} \leq e^{\frac{1}{12\ell}}$ which implies $\ell! \in (1 \pm \frac{1}{\ell})\sqrt{2\pi\ell} \cdot \ell^\ell \cdot e^{-\ell}$. Compute

$$\begin{aligned}
\binom{2m}{m+k} &= \frac{(2m)!}{(m+k)!(m-k)!} \\
&\in \frac{(1 \pm \frac{1}{2m})\sqrt{2\pi \cdot 2m}(2m)^{2m}e^{-2m}}{(1 \pm \frac{1}{m+k})\sqrt{2\pi(m+k)}(m+k)^{m+k}e^{-(m+k)} \cdot (1 \pm \frac{1}{m-k})\sqrt{2\pi(m-k)}(m-k)^{m-k}e^{-(m-k)}} \\
&\subseteq \frac{\sqrt{2\pi \cdot 2m}(2m)^{2m}e^{-2m}}{\sqrt{2\pi(m+k)}(m+k)^{m+k}e^{-(m+k)} \cdot \sqrt{2\pi(m-k)}(m-k)^{m-k}e^{-(m-k)}} \cdot (1 \pm \frac{20}{m}) \\
&= \frac{(2m)^{2m+\frac{1}{2}}}{\sqrt{2\pi} \cdot (m+k)^{m+k+\frac{1}{2}} \cdot (m-k)^{m-k+\frac{1}{2}}} \cdot (1 \pm \frac{20}{m}) \\
&= 2^{2m} \cdot \frac{1}{\sqrt{\pi m} \cdot (1+\frac{k}{m})^{m+k+\frac{1}{2}} \cdot (1-\frac{k}{m})^{m-k+\frac{1}{2}}} \cdot (1 \pm \frac{20}{m}) \\
&= 2^{2m} \cdot \frac{1}{\sqrt{\pi m} \cdot (1-\frac{k^2}{m^2})^{m-k+\frac{1}{2}} \cdot (1+\frac{k}{m})^{2k}} \cdot (1 \pm \frac{20}{m}),
\end{aligned}$$

[**Eliad's Note: Ask Iftach what word needs to replace the word "equality"**] where the first containment holds since $m \geq 100$ and $|k| \leq m^{\frac{3}{5}}$ implies $\frac{(1\pm\frac{1}{m})}{(1\pm\frac{1}{m+k})(1\pm\frac{1}{m-k})} \subseteq (1 \pm \frac{20}{m})$.

Since $1+x \in e^{x \pm x^2}$ for $x \in (-0.5, 0.5)$, it holds that

$$\begin{aligned}
\binom{2m}{m+k} \cdot 2^{-2m} &\in \frac{1}{\sqrt{\pi m} \cdot e^{(-\frac{k^2}{m^2} \pm \frac{k^4}{m^4})(m-k+\frac{1}{2})} \cdot e^{(\frac{k}{m} \pm \frac{k^2}{m^2}) \cdot 2k}} \cdot (1 \pm \frac{20}{m}) \\
&= \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot e^{-\frac{k^3}{m^2} \pm \frac{2k^3}{m^2} + \frac{k^2}{2m^2} \pm \frac{k^4}{m^4}(m-k+\frac{1}{2})} \cdot (1 \pm \frac{20}{m}) \\
&\subseteq \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot e^{\pm \frac{4|k|^3}{m^2}} \cdot (1 \pm \frac{20}{m}) \\
&\subseteq \frac{1}{\sqrt{\pi m}} \cdot e^{-\frac{k^2}{m}} \cdot (1 \pm \frac{8\,|k|^3}{m^2}) \cdot (1 \pm \frac{20}{m}) \\
&\subseteq \frac{1}{\sqrt{\pi}} \cdot \left(1 \pm 20 \cdot (\frac{|k|^3}{m^2} + \frac{1}{m})\right) \cdot \frac{1}{\sqrt{m}} \cdot e^{-\frac{k^2}{m}}.
\end{aligned} \tag{51}$$

The first containment holds since $-\frac{k^3}{m^2} \pm \frac{2k^3}{m^2} + \frac{k^2}{2m^2} \pm \frac{k^4}{m^4}(m-k+\frac{1}{2}) \subseteq [-\frac{4|k|^3}{m^2}, \frac{4|k|^3}{m^2}]$. Since $e^x \in 1 \pm 2x$ for every $|x| < 1$, it holds that $e^{\pm \frac{4|k|^3}{m^2}} \subseteq (1 \pm \frac{8|k|^3}{m^2})$ which yields the second containment. [**Eliad's Note: Check the explanation**] □

Proposition A.3 (Restatement of Proposition 2.14)**.** *Let $n \in \mathbb{N}$, $t \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$ with $|t| \le n^{\frac{3}{5}}$, $|\varepsilon| \le n^{-\frac{2}{5}}$ and $\frac{n+t}{2} \in \mathbb{N}$. Then*

$$\mathcal{B}_{n,\varepsilon}(t) \in (1 \pm \mathsf{error}) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

where $\mathsf{error} = \xi \cdot (\varepsilon^2 |t| + \frac{1}{n} + \frac{|t|^3}{n^2} + \epsilon^4 n)$ *for some universal constant* $\xi \ge 0$.

Proof. Compute

$$\begin{aligned}
\mathcal{B}_{n,\varepsilon}(t) &= \binom{n}{\frac{n+t}{2}} 2^{-n} (1+\varepsilon)^{\frac{n+t}{2}} (1-\varepsilon)^{\frac{n-t}{2}} \\
&\in \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} e^{-\frac{t^2}{2n}} \cdot (1-\varepsilon^2)^{\frac{n-t}{2}} (1+\varepsilon)^t,
\end{aligned} \tag{52}$$

where ξ_1 is the universal constant from Proposition A.2. The first belonging holds by Proposition A.2. Since $1+x \in e^{x \pm x^2}$ for $x \in (-0.5, 0.5)$, it follows that:

$$\begin{aligned}
\mathcal{B}_{n,\varepsilon}(t) &\in \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{t^2}{2n}} e^{(-\varepsilon^2 \pm \varepsilon^4) \cdot \frac{n-t}{2}} e^{(\varepsilon \pm \varepsilon^2) t} \\
&\subseteq \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} e^{-\frac{t^2}{2n} - \frac{\varepsilon^2 n}{2} + \varepsilon t} \cdot e^{\pm (2\varepsilon^2 |t| + \frac{\varepsilon^4 n}{2})} \\
&\subseteq \sqrt{\frac{2}{\pi}} (1 \pm \xi_1 \cdot (\frac{|t|^3}{n^2} + \frac{1}{n})) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}} (1 \pm 4 \cdot (\varepsilon^2 |t| + \epsilon^4 n)) \\
&\subseteq \sqrt{\frac{2}{\pi}} (1 \pm \xi \cdot (\varepsilon^2 |t| + \frac{|t|^3}{n^2} + \frac{1}{n} + \epsilon^4 n)) \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},
\end{aligned}$$

where $\xi = 2 \cdot (\xi_1 + 4)$. The second containment holds since $2\varepsilon^2 |t| + \frac{\varepsilon^4 n}{2} < 1$ and since $e^x = 1 \pm 2x$ for $x \in (-1, 1)$. [**Eliad's Note: Check the explanation**] □

[Iftach's Note: add motivation]

Fact A.4 ([1]). *For $x \geq 0$, it holds that*

$$\sqrt{\frac{2}{\pi}} \cdot \frac{e^{-\frac{x^2}{2}}}{x + \sqrt{x^2+4}} \leq \Phi(x) \leq \sqrt{\frac{2}{\pi}} \cdot \frac{e^{-\frac{x^2}{2}}}{x + \sqrt{x^2 + \frac{8}{\pi}}}.$$

Proposition A.5. *For $n \in \mathbb{N}$, $\varepsilon \in (-1,1)$ and $k, k' \in \mathbb{Z}$ such that $k' \geq k \geq \varepsilon n$, it holds that*

$$\left| \sum_{t=k}^{k'} e^{-\frac{(t-\varepsilon n)^2}{2n}} - \int_k^{k'} e^{-\frac{(t-\varepsilon n)^2}{2n}} dt \right| \leq e^{-\frac{(k-\varepsilon n)^2}{2n}}.$$

Proof. Consider the function $f(t) = e^{-\frac{(t-\varepsilon n)^2}{2n}}$. The function f obtains its maximum at $t = \varepsilon n$ and is monotonic decreasing in $[\varepsilon n, \infty)$. In particular, it is decreasing in $[k, \infty)$. Since $\sum_{t=k}^{k'} f(t)$ is an upper Darboux sum of f with respect to $\{k, k+1, \ldots, k'+1\}$, it holds that $\int_k^{k'} f(t)dt \leq \int_k^{k'+1} f(t)dt \leq \sum_{t=k}^{k'} f(t)$. In addition, since $\sum_{t=k+1}^{k'} f(t)$ is a lower Darboux sum of f with respect to $\{k, k+1, \ldots, k'\}$, it holds that $\sum_{t=k}^{k'} f(t) \leq \int_k^{k'} f(t)dt + f(k)$. The proof follows, since the difference between the above sums is at most $f(k) = e^{-\frac{(k-\varepsilon n)^2}{2n}}$. □

Proposition A.6. *There exists $\varphi \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $k \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$, with $|\varepsilon| \leq c \cdot \sqrt{\frac{\log n}{n}}$ and $|k| < c \cdot \sqrt{n \log n}$, for some $c \geq 1$. Then*

$$\widehat{\mathsf{B}}_{n,\varepsilon}(k) \in \Phi(\frac{k - \varepsilon n}{\sqrt{n}}) \pm \varphi(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}$$

Proof. There exists a function $\vartheta \colon \mathbb{R}^+ \mapsto \mathbb{N}$ such that $n^{\frac{3}{5}} > c \cdot \sqrt{n \log n}$ for every $n \geq \vartheta(c)$. In the following we focus on $n \geq \vartheta(c)$, where smaller n's are handled by setting the value of $\varphi(c)$ to be large enough on those values. We also assume for simplicity that n and k are both even, the proofs of the other cases are analogous. Let ξ_1 be the constant defined in Proposition A.3, and let $\ell = 4c \cdot \sqrt{n \log n}$. We start by handling the case $k \geq \varepsilon n$.

It holds that

$$\begin{aligned}
\sum_{t=k}^{\ell} \mathcal{B}_{n,\varepsilon}(t) &= \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \mathcal{B}_{n,\varepsilon}(2t) \qquad (53)\\
&\in \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\varepsilon^2 |2t| + \frac{|2t|^3}{n^2} + \frac{1}{n} + \varepsilon^4 n)) \cdot \frac{1}{\sqrt{n}} e^{-\frac{(2t-\varepsilon n)^2}{2n}} \\
&\subseteq \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}}(1 \pm \varphi'(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}}) \cdot \frac{1}{\sqrt{n}} e^{-\frac{(2t-\varepsilon n)^2}{2n}} \\
&\subseteq (1 \pm \varphi'(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}}) \cdot A(n,k,\varepsilon,c),
\end{aligned}$$

letting $\varphi'(c) := \xi_1 \cdot (c^4 + 520c^3 + 1)$ and $A(n,k,\varepsilon,c) := \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t-\varepsilon n)^2}{2n}}$. The first equality holds since $\mathcal{B}_{n,\varepsilon}(j) = 0$ for every odd j, the first belonging holds by Proposition A.3 and it is easy to verify that the first containment holds for the given values of n, ε and k.

Compute

$$\begin{aligned}
A(n,k,\varepsilon,c) &= \sum_{t=\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t-\varepsilon n)^2}{2n}} \\
&\in \int_{\frac{k}{2}}^{\frac{\ell}{2}} \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(2t-\varepsilon n)^2}{2n}} dt \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \\
&= \int_{\frac{k-\varepsilon n}{\sqrt{n}}}^{\frac{\ell-\varepsilon n}{\sqrt{n}}} \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{x^2}{2}} dx \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \\
&= \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) - \Phi(\frac{\ell-\varepsilon n}{\sqrt{n}}) \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \\
&\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{1}{n^{4c^2}} \pm \frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \\
&\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}.
\end{aligned} \tag{54}$$

Since $k \geq \varepsilon n$, the first belonging holds by [**Eliad's Note: Change Proposition A.5**] Proposition A.5. The second equality holds by letting $x = \frac{2t-\varepsilon n}{\sqrt{n}}$. The first containment holds since [**Iftach's Note: separate**] $\Phi(\frac{\ell-\varepsilon n}{\sqrt{n}}) \leq \Phi(3c\sqrt{\log n}) \leq \frac{1}{n^{4c^2}}$ by Fact A.4. Finally, the second containment holds since $|k - \varepsilon n| \leq 2c \cdot \sqrt{n \log n}$, and therefore $\frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \geq \frac{1}{n^{2c^2+\frac{1}{2}}} \geq \frac{1}{n^{4c^2}}$. It follows that

$$\begin{aligned}
\sum_{t=k}^{\ell} \mathcal{B}_{n,\varepsilon}(t) &\in (1 \pm \varphi'(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}}) \cdot (\Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}) \\
&= \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi'(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm 2 \cdot \varphi'(c) \cdot \frac{\log^{1.5}(n)}{n} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \pm \frac{2}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \\
&\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi''(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},
\end{aligned} \tag{55}$$

letting $\varphi''(c) := 3 \cdot \varphi'(c) + 2$. We conclude that

$$\begin{aligned}
\widehat{\mathsf{B}}_{n,\varepsilon}(k) &= \sum_{t=k}^{n} \mathcal{B}_{n,\varepsilon}(t) \\
&= \sum_{t=k}^{\ell} \mathcal{B}_{n,\varepsilon}(t) + \Pr_{x \leftarrow \mathcal{B}_{n,\varepsilon}}[x > \ell] \\
&\in \left(\Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm \varphi''(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \right) \pm \frac{1}{n^{4c^2}} \\
&\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm (\varphi''(c) + 1) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},
\end{aligned} \tag{56}$$

where the first belonging holds by Equation (55) and by Hoeffding's inequality (see Fact 2.12).

It is left to handel the case $k < \varepsilon n$. For such k, it holds that

$$\begin{aligned}\widehat{\mathsf{B}}_{n,\varepsilon}(k) &= 1 - \widehat{\mathsf{B}}_{n,-\varepsilon}(-k) + \mathcal{B}_{n,\varepsilon}(k) \\ &\in \left(1 - \Phi(\frac{-k+\varepsilon n}{\sqrt{n}}) \pm (\varphi''(c)+1) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\right) \pm \left(\frac{1}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\right) \\ &\subseteq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \pm (\varphi''(c)+2) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}},\end{aligned} \tag{57}$$

where the first belonging holds by Equation (56) applied to $-k$ and $-\varepsilon$, and by evaluating the value of $\mathcal{B}_{n,\varepsilon}(k)$ using Proposition A.3.[**Iftach's Note: split**] □

Proposition A.7 (Restatement of Proposition 2.15)**.** *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $t, x, x' \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ be with $|x|, |x'|, |t| \leq c \cdot \sqrt{n \log n}$ and $|\varepsilon| \leq c \cdot \sqrt{\frac{\log n}{n}}$, for some $c \geq 1$, then*

$$\frac{\mathcal{B}_{n,\varepsilon}(t-x')}{\mathcal{B}_{n,\varepsilon}(t-x)} \in \exp\left(\frac{-2\cdot(t-\varepsilon n)\cdot x + x^2 + 2\cdot(t-\varepsilon n)\cdot x' - x'^2}{2n}\right) \cdot \left(1 \pm \varphi(c) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right).$$

Proof. Let φ_1 be the function from Proposition A.3 and let $\varphi_2(c) = 4 \cdot \varphi_1(c) \cdot (10c^3+1)$. It holds that

$$\begin{aligned}\frac{\mathcal{B}_{n,\varepsilon}(t-x')}{\mathcal{B}_{n,\varepsilon}(t-x)} &\in \frac{\left(1 \pm \varphi_1(c)\cdot(\varepsilon^2|t-x'| + \frac{1}{n} + \frac{|t-x'|^3}{n^2})\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x')^2}{2n}}}{\left(1 \pm \varphi_1(c)\cdot(\varepsilon^2|t-x| + \frac{1}{n} + \frac{|t-x|^3}{n^2})\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x)^2}{2n}}} \\ &\subseteq \frac{\left(1 \pm \varphi_1(c)\cdot(10c^3+1)\cdot\frac{\log^{1.5}(n)}{\sqrt{n}}\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x')^2}{2n}}}{\left(1 \pm \varphi_1(c)\cdot(10c^3+1)\cdot\frac{\log^{1.5}(n)}{\sqrt{n}}\right) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n - x)^2}{2n}}} \\ &\subseteq \exp\left(\frac{(t-\varepsilon n - x)^2}{2n} - \frac{(t-\varepsilon n - x')^2}{2n}\right) \cdot (1 \pm \varphi_2(c)\cdot\frac{\log^{1.5}(n)}{\sqrt{n}}) \\ &= \exp\left(\frac{-2\cdot(t-\varepsilon n)\cdot x + x^2 + 2\cdot(t-\varepsilon n)\cdot x' - x'^2}{2n}\right) \cdot (1 \pm \varphi_2(c)\cdot\frac{\log^{1.5}(n)}{\sqrt{n}}),\end{aligned}$$

The first belonging holds by Proposition A.3, and the first containment by the assumption on $|t|$, $|x|$, $|x'|$ and $|\varepsilon|$. □

Proposition A.8 (Restatement of Proposition 2.16)**.** *For $n \in \mathbb{N}$, $k, k' \in \mathbb{Z}$ and $\varepsilon \in [-1,1]$, where n is larger than a universal constant, $|k|, |k'| \leq \log(n) \cdot \sqrt{n \log n}$ and $|\varepsilon| \leq \log(n) \cdot \sqrt{\frac{\log n}{n}}$, it holds that*

$$\left|\widehat{\mathsf{B}}_{n,\varepsilon}(k) - \widehat{\mathsf{B}}_{n,\varepsilon}(k')\right| \leq \frac{|k-k'|}{\sqrt{n}}$$

Proof. By Proposition A.3, for every $t \in \mathbb{Z}$ with $|t| \leq \log(n) \cdot \sqrt{n \log n}$, it holds that

$$\mathcal{B}_{n,\varepsilon}(t) \in (1 \pm 0.1) \cdot \sqrt{\frac{2}{\pi}} \cdot \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}},$$

and therefore

$$\mathcal{B}_{n,\varepsilon}(t) \leq \frac{1}{\sqrt{n}} \cdot e^{-\frac{(t-\varepsilon n)^2}{2n}} \leq \frac{1}{\sqrt{n}}.$$

Assume without loss of generality that $k' \geq k$, it holds that $\widehat{\mathsf{B}}_{n,\varepsilon}(k) - \widehat{\mathsf{B}}_{n,\varepsilon}(k') = \sum_{t=k}^{k'} \mathcal{B}_{n,\varepsilon}(t)$, which by the bound above, is at most $\frac{(k'-k)}{\sqrt{n}}$. □

Proposition A.9 (Restatement of Proposition 2.17)**.** *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $c, n, n' \in \mathbb{N}$, $k \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$, such that $c > 10$, $n \leq n'$, $|k| \leq c \cdot \sqrt{n \log n}$, $|\varepsilon| \leq c \cdot \sqrt{\frac{\log n}{n}}$, and $\log^{\frac{1}{2}}(n) \geq \max\{8 \cdot \varphi(3c), c\}$. then $\left|\mathcal{B}^{-1}(n, \varepsilon, k, n') - \frac{\varepsilon n - k}{\sqrt{n \cdot n'}}\right| \leq \frac{\log^2 n}{\sqrt{n \cdot n'}}$.*[**Iftach's Note:** $B^{-1}(n, \varepsilon, n', k)$]

Proof. Let φ be the function from Proposition A.6 and let $\varepsilon^+ = -\frac{k-\varepsilon n}{\sqrt{n \cdot n'}} + \frac{\log^2 n}{\sqrt{n \cdot n'}}$ and $\varepsilon^- = -\frac{k-\varepsilon n}{\sqrt{n \cdot n'}} - \frac{\log^2 n}{\sqrt{n \cdot n'}}$. We prove that $\varepsilon^- < \mathcal{B}^{-1}(n, \varepsilon, k, n') < \varepsilon^+$, yielding the required bound. For simplicity, we focus on the upper bound, whereas the lower bound can be proven analogously.

Since $|\varepsilon^+| < 3c \cdot \sqrt{\frac{\log n'}{n'}}$, Proposition A.6 yields that

$$\begin{aligned}
\widehat{\mathsf{B}}_{n',\varepsilon^+}(0) &\in \Phi(-\varepsilon^+ \cdot \sqrt{n'}) \pm \varphi(3c) \cdot \frac{\log^{\frac{3}{2}} n'}{\sqrt{n'}} \cdot e^{-\frac{\varepsilon^{+2} \cdot n'}{2}} \\
&= \Phi\left(\frac{k - \varepsilon n - \log^2 n}{\sqrt{n \cdot n'}} \cdot \sqrt{n'}\right) \pm \varphi(3c) \cdot \frac{\log^{\frac{3}{2}} n'}{\sqrt{n'}} \cdot e^{-\frac{1}{2} \cdot \left(\frac{k - \varepsilon n - \log^2 n}{\sqrt{n \cdot n'}}\right)^2 \cdot n'} \\
&= \Phi\left(\frac{k - \varepsilon n - \log^2 n}{\sqrt{n}}\right) \pm \varphi(3c) \cdot \frac{\log^{\frac{3}{2}} n'}{\sqrt{n'}} \cdot e^{-\frac{(k - \varepsilon n - \log^2 n)^2}{2n}}.
\end{aligned} \tag{58}$$

Since $\log n > c$ and $|k - \varepsilon n| \leq 2c\sqrt{n \log n}$, for every $a \in [0, \log^2 n]$ it holds that $e^{-\frac{(k-\varepsilon n-a)^2}{2n}} = e^{-\frac{(k-\varepsilon n)^2}{2n}}(1 \pm \frac{\log^3 n}{\sqrt{n}})$, yielding that [**Iftach's Note: equation**] $\Phi(\frac{k-\varepsilon n-\log^2 n}{\sqrt{n}}) = \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) + \frac{1}{\sqrt{2\pi}} \cdot \int_{\frac{k-\varepsilon n-\log^2 n}{\sqrt{n}}}^{\frac{k-\varepsilon n}{\sqrt{n}}} e^{-\frac{x^2}{2}} dx \geq \Phi(\frac{k-\varepsilon n}{\sqrt{n}}) + \frac{1}{\sqrt{2\pi}} \cdot \frac{\log^2 n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}(1 - \frac{\log^3 n}{\sqrt{n}})$ and $e^{-\frac{(k-\varepsilon n-\log^2 n)^2}{2n}} \leq e^{-\frac{(k-\varepsilon n)^2}{2n}}(1 + \frac{\log^3 n}{\sqrt{n}})$. Therefore, it holds that

$$\begin{aligned}
&\widehat{\mathsf{B}}_{n',\varepsilon^+}(0) \\
&\geq \Phi\left(\frac{k - \varepsilon n}{\sqrt{n}}\right) + \frac{1}{\sqrt{2\pi}} \cdot \frac{\log^2 n}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\left(1 - \frac{\log^3 n}{\sqrt{n}}\right) - \varphi(3c) \cdot \frac{\log^{\frac{3}{2}} n'}{\sqrt{n'}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\left(1 + \frac{\log^3 n}{\sqrt{n}}\right) \\
&\geq \Phi\left(\frac{k - \varepsilon n}{\sqrt{n}}\right) + \frac{\log^2 n}{2\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\left(1 - \frac{\log^3 n}{\sqrt{n}}\right) - \varphi(3c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\left(1 + \frac{\log^3 n}{\sqrt{n}}\right) \\
&\geq \Phi\left(\frac{k - \varepsilon n}{\sqrt{n}}\right) + \frac{\log^2 n}{4\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}}\left(1 - \frac{\log^3 n}{\sqrt{n}}\right) \\
&\geq \widehat{\mathsf{B}}_{n,\varepsilon}(k).
\end{aligned} \tag{59}$$

The second inequality holds since $n' \geq n$ and $\sqrt{2\pi} \geq 2$. The third inequality holds since $\log^{\frac{1}{2}} n \geq 8 \cdot \varphi(3c)$ and therefore $\frac{\log^2 n}{4\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \cdot (1 - \frac{\log^3 n}{\sqrt{n}}) \geq \varphi(3c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} (1 + \frac{\log^3 n}{\sqrt{n}})$. The last inequality holds since by Proposition A.6 $\Phi(\frac{k-\varepsilon n}{\sqrt{n}}) \in \widehat{\mathsf{B}}_{n,\varepsilon}(k) \pm \mathsf{error}$, where $\mathsf{error} = \varphi(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} \leq \frac{\log^2 n}{4\sqrt{n}} \cdot e^{-\frac{(k-\varepsilon n)^2}{2n}} (1 - \frac{\log^3 n}{\sqrt{n}})$.

□

Recall that for $i, n \in \mathbb{N}$ with $i \leq n$, we let $\ell_n(i) = n - i + 1$ and let $\mathsf{sum}_n(i) = \sum_{j=i}^{n} \ell_n(i) = \frac{1}{2} \cdot \ell_n(i)(\ell_n(i) + 1)$.

[**Iftach's Note: motivation**]

Proposition A.10. *There exists $\varphi \colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n, i \in \mathbb{N}$, $x, \beta, \alpha \in \mathbb{Z}$ and $\varepsilon \in [-1, 1]$ be such that $i \leq n - \log^{1.5} n$, $|\alpha| \leq \sqrt{c \cdot \mathsf{sum}_n(i) \cdot \log n}$, $|x| \leq \sqrt{c \cdot \ell_n(i) \cdot \log \ell_n(i)}$, $|\beta| \leq \sqrt{c}$ and $|\varepsilon| \leq \sqrt{c \cdot \frac{\log n}{\mathsf{sum}_n(i)}}$, for some $c \geq 0$, then:*

$$\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)}\right) \in 1 \pm \varphi(c) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)}.$$

Proof. There exists integer function φ', such that $\left|\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)}\right| < 1$ for every $n > \varphi'(c)$ [**Iftach's Note: explain**]

In the following we assume $n > \varphi'(c)$, where for smaller values of n ,,,

For such n, it holds that

$$\begin{aligned}
\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)}\right) &\in 1 \pm 2 \cdot \left|\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)}\right| \\
&\subseteq 1 \pm 2 \cdot \left(\frac{|\alpha| \cdot |x| + |\beta| \cdot x^2}{\mathsf{sum}_n(i)}\right) \\
&\subseteq 1 \pm 2 \cdot \left(\frac{\sqrt{c \cdot \mathsf{sum}_n(i) \cdot \log n} \cdot |x| + \sqrt{c} \cdot x^2}{\mathsf{sum}_n(i)}\right) \\
&\subseteq 1 \pm 2 \cdot \left(\sqrt{\frac{c \cdot \log n}{\mathsf{sum}_n(i)}} \cdot |x| + \frac{\sqrt{c}}{\mathsf{sum}_n(i)} \cdot \sqrt{c \cdot \ell_n(i) \cdot \log \ell_n(i)} \cdot |x|\right) \\
&= 1 \pm 2 \cdot \left(\sqrt{\frac{c \cdot \log n}{\frac{1}{2}\ell_n(i)(\ell_n(i)+1)}} \cdot |x| + \frac{c \cdot \sqrt{\ell_n(i) \cdot \log \ell_n(i)}}{\frac{1}{2}\ell_n(i)(\ell_n(i)+1)} \cdot |x|\right) \\
&\subseteq 1 \pm 4c \cdot \sqrt{\frac{\log n}{\ell_n(i)}} \left(\frac{|x|}{\sqrt{\ell_n(i)}} + \frac{|x|}{\ell_n(i)}\right) \\
&\subseteq 1 \pm 8c \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)},
\end{aligned}$$

[**Iftach's Note:**] where the first belonging holds since $e^y \in 1 \pm 2|y|$ for $y \in [-1, 1]$, the second containment holds by taking the maximum possible values of $|\alpha|$ and $|\beta|$, the third one by taking the maximum possible values of $|x|$ and the first equality holds by the definition of $\mathsf{sum}_n(i)$. □

Using the above fact, we can prove Proposition 2.19.

Proposition A.11 (Restatement of Proposition 2.19)**.** *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds. For every $n, i \in \mathbb{N}$, $x, \beta, \beta', \alpha, \alpha' \in \mathbb{Z}$, $\varepsilon \in [-1,1]$ and $\mathcal{S} \subseteq \mathbb{Z}$, such that $i \leq n - \log^{1.5} n$, $|\alpha|, |\alpha'| \leq \sqrt{c \cdot \mathsf{sum}_n(i) \cdot \log n}$, $|\beta|, |\beta'| \leq \sqrt{c}$, $|x| \leq \sqrt{c \cdot \ell_n(i) \cdot \log \ell_n(i)}$, $|\varepsilon| \leq \sqrt{c \cdot \frac{\log n}{\mathsf{sum}_n(i)}}$, for some $c \geq 0$, and $\mathrm{E}_{x' \leftarrow \mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}[|x'|] \leq \mathrm{E}_{x' \leftarrow \mathcal{B}_{\ell_n(i),\varepsilon}}[|x'|]$,[23] it holds that:*

$$\mathop{\mathrm{E}}_{x' \leftarrow \mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}\left[\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2 + \alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i)}\right)\right] \in 1 \pm \varphi(c) \cdot \sqrt{\frac{\log n}{\ell_n(i)}}\left(1 + \frac{|x|}{\sqrt{\ell_n(i)}}\right).$$

Proof.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{x' \leftarrow \mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}\left[\exp\left(\frac{\alpha \cdot x + \beta \cdot x^2 + \alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i)}\right)\right] \\
&= \exp\left(\frac{\alpha \cdot x + \beta \cdot x^2}{\mathsf{sum}_n(i)}\right) \cdot \mathop{\mathrm{E}}_{x' \leftarrow \mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}\left[\left(\frac{\alpha' \cdot x' + \beta' \cdot x'^2}{\mathsf{sum}_n(i)}\right)\right] \\
&\in (1 \pm \varphi_1(c) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)}) \cdot \mathop{\mathrm{E}}_{x' \leftarrow \mathcal{B}^{\mathcal{S}}_{\ell_n(i),\varepsilon}}\left[1 \pm \varphi_1(c) \cdot \frac{\sqrt{\log n} \cdot |x'|}{\ell_n(i)}\right] \\
&= (1 \pm \varphi_1(c) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)}) \cdot (1 \pm \varphi_1(c) \cdot \frac{\sqrt{\log n} \cdot \mathrm{E}_{x'}[|x'|]}{\ell_n(i)}) \\
&\subseteq (1 \pm \varphi_1(c) \cdot \frac{\sqrt{\log n} \cdot |x|}{\ell_n(i)}) \cdot (1 \pm 2\varphi_1(c) \cdot \sqrt{\frac{\log n}{\ell_n(i)}}) \\
&\subseteq 1 \pm 2\varphi_1(c) \cdot \sqrt{\frac{\log n}{\ell_n(i)}}(1 + \frac{|x|}{\sqrt{\ell_n(i)}}),
\end{aligned}$$

where φ_1 is the function from Proposition A.10. The first belonging holds by Proposition A.10, and the first containment by Fact 2.13. □

A.3 Facts About the Hypergeometric Distribution

[**Iftach's Note: motivation**] [**Iftach's Note: change other statements to this form**]

Proposition A.12. *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $p, t \in \mathbb{Z}$ and $c > 0$ be such that $\left|\frac{p}{n}\right| < 1$, $|t| \leq n^{3/5}$ and $|p| \leq c \cdot \sqrt{\frac{\log n}{n}}$, then*

$$\mathcal{HG}_{2n,p,n}(t) \in \mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t) \cdot (1 \pm \mathsf{error}),$$

for $\mathsf{error} = \varphi(c) \cdot (\frac{n + |p|^3 + |t|^3}{n^2})$.

[23] Recall that $X^{\mathcal{S}}$, where X is a random variable and $\mathcal{S}$ is a set, denotes a random sample according to X, conditioned on $X \in \mathcal{S}$.

Proof. [**Iftach's Note: check notation**] Let $\omega = \frac{p}{2}$. Note that number of ones in a set $\mathcal{S}$ over $\{-1,1\}$ of size $2n$ and $w(\mathcal{S}) = p$, is $n+\omega$. It follows that

$$\begin{aligned}
\mathcal{HG}_{2n,p,n}(t) &= \frac{\binom{n+\omega}{\frac{n+t}{2}} \cdot \binom{n-\omega}{\frac{n-t}{2}}}{\binom{2n}{n}} \\
&= \frac{\binom{n+\omega}{\frac{n+\omega}{2}+\frac{t-\omega}{2}} \cdot \binom{n-\omega}{\frac{n-\omega}{2}-\frac{t-\omega}{2}}}{\binom{2n}{n}} \\
&\in \frac{\sqrt{\frac{2}{\pi}}(1 \pm \xi_1 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2})) \frac{1}{\sqrt{n+\omega}} e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot \sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_1 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2})) \frac{1}{\sqrt{n-\omega}} e^{-\frac{(t-\omega)^2}{2(n-\omega)}}}{\sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_1 \cdot \frac{1}{n}) \frac{1}{\sqrt{2n}}} \\
&\subseteq \sqrt{\frac{2}{\pi}} \cdot (1 \pm \xi_2 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2})) \cdot A(n,t,\omega),
\end{aligned}$$

where ξ_1 is the constant from Proposition A.2, [**Iftach's Note: ..**] ξ_2 is a universal constant such that $\frac{(1\pm\xi_1\cdot(\frac{1}{n}+\frac{|t-\omega|^3}{n^2}))\cdot(1\pm\xi_1\cdot(\frac{1}{n}+\frac{|t-\omega|^3}{n^2}))}{(1\pm\xi_1\cdot\frac{1}{n})} \subseteq (1 \pm \xi_2 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2}))$, and $A(n,t,\omega) = \frac{\frac{1}{\sqrt{n+\omega}} e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot \frac{1}{\sqrt{n-\omega}} e^{-\frac{(t-\omega)^2}{2(n-\omega)}}}{\frac{1}{\sqrt{2n}}}$. In addition, the first belonging holds by Proposition A.2. It follows that

$$\begin{aligned}
A(n,t,\omega) &= \sqrt{\frac{2}{n}} \cdot \frac{n}{\sqrt{n+\omega} \cdot \sqrt{n-\omega}} \cdot e^{-\frac{(t-\omega)^2}{2(n+\omega)}} \cdot e^{-\frac{(t-\omega)^2}{2(n-\omega)}} \\
&= \sqrt{\frac{2}{n}} \cdot \frac{1}{\sqrt{1-\frac{\omega^2}{n^2}}} \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot e^{-(t-\omega)^2(\frac{1}{2(n+\omega)}+\frac{1}{2(n-\omega)}-\frac{1}{n})} \\
&\in \sqrt{\frac{2}{n}} \cdot (1 \pm 2 \cdot \frac{\omega^2}{n^2}) \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot e^{-\frac{(t-\omega)^2\omega^2}{n(n^2-\omega^2)}} \\
&\subseteq \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}} \cdot (1 \pm \varphi_1(c) \cdot (\frac{(t-\omega)^2\omega^2}{n^3} + \frac{\omega^2}{n^2})),
\end{aligned}$$

where φ_1 is a universal function such that $(1 \pm 2 \cdot \frac{\omega^2}{n^2}) \cdot e^{-\frac{(t-\omega)^2\omega^2}{n(n^2-\omega^2)}} \subseteq (1 \pm \varphi_1(c) \cdot (\frac{(t-\omega)^2\omega^2}{n^3} + \frac{\omega^2}{n^2}))$. The third equality holds by the fact that $\left|\frac{p}{n}\right| < 1 \Rightarrow \frac{\omega^2}{n^2} < \frac{1}{4}$, and for $x \in [0, \frac{1}{4}]$ it holds that $\frac{1}{\sqrt{1-x}} \in 1 \pm 2x$.

By taking a universal function ξ_4 such that $(1 \pm \xi_2 \cdot (\frac{1}{n} + \frac{|t-\omega|^3}{n^2})) \cdot (1 \pm \varphi_1(c) \cdot (\frac{(t-\omega)^2\omega^2}{n^3} + \frac{\omega^2}{n^2})) \subseteq$

$(1 \pm \varphi_2(c) \cdot (\frac{n+|\omega|^3+|t|^3}{n^2}))$, it holds that:

$$\begin{aligned}
\mathcal{HG}_{2n,p,n}(t) &\in \sqrt{\frac{2}{\pi}} \cdot (1 \pm \varphi_2(c) \cdot (\frac{n+|\omega|^3+|t|^3}{n^2})) \cdot \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}} \\
&= \frac{\sqrt{\frac{2}{\pi}} \cdot (1 \pm \varphi_2(c) \cdot (\frac{n+|\omega|^3+|t|^3}{n^2})) \cdot \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}}}{\mathcal{B}_{\frac{n}{2},\frac{2\omega}{n}}(t)} \cdot \mathcal{B}_{\frac{n}{2},\frac{2\omega}{n}}(t) \\
&\subseteq \frac{\sqrt{\frac{2}{\pi}} \cdot (1 \pm \varphi_2(c) \cdot (\frac{n+|\omega|^3+|t|^3}{n^2})) \cdot \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}}}{\sqrt{\frac{2}{\pi}} \cdot (1 \pm \varphi_3(c)(\frac{\omega^2|t|}{n} + \frac{1}{n} + \frac{|t|^3}{n^2})) \cdot \sqrt{\frac{2}{n}} \cdot e^{-\frac{(t-\omega)^2}{n}}} \cdot \mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t) \\
&\subseteq (1 \pm \varphi_4(c)(\frac{n+|p|^3+|t|^3}{n^2})) \cdot \mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t),
\end{aligned}$$

where φ_3 is the function from Proposition A.3 and φ_4 is a universal function such that $\frac{1\pm\varphi_2(c)\cdot(\frac{n+|\omega|^3+|t|^3}{n^2})}{1\pm\varphi_3(c)(\frac{\omega^2|t|}{n}+\frac{1}{n}+\frac{|t|^3}{n^2})} \subseteq 1 \pm \varphi_4(c)(\frac{n+|p|^3+|t|^3}{n^2})$. In addition, the first containment holds by Proposition A.3. □

Proposition A.13 (Restatement of Proposition 2.21)**.** *There exists $\varphi\colon \mathbb{R}^+ \mapsto \mathbb{R}^+$ such that the following holds: let $n \in \mathbb{N}$, $p, t, x, x' \in \mathbb{Z}$ and $c \geq 0$ be such that $\left|\frac{p}{n}\right| < 1$ and $|p|, |t|, |x|, |x'| \leq c \cdot \sqrt{n \log n}$, then*

$$\frac{\mathcal{HG}_{2n,p,n}(t-x')}{\mathcal{HG}_{2n,p,n}(t-x)} \in \exp\left(\frac{-2(t-p)x + x^2 + 2(t-p)x' - x'^2}{n}\right) \cdot \left(1 \pm \varphi(c) \cdot \frac{\log^{1.5} n}{\sqrt{n}}\right).$$

Proof. Proposition A.12 yields that there exists a universal function φ_1, such that

$$\frac{\mathcal{HG}_{2n,p,n}(t-x')}{\mathcal{HG}_{2n,p,n}(t-x)} \in \frac{\mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t-x') \cdot (1 \pm \varphi_1(c) \cdot (\frac{n+|p|^3+|t-x'|^3}{n^2}))}{\mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t-x) \cdot (1 \pm \varphi_1(c) \cdot (\frac{n+|p|^3+|t-x|^3}{n^2}))} \tag{60}$$

[**Iftach's Note: ..**] The bounds on p, t, x and x', yields that for some universal function φ_2, it holds that

$$\frac{\mathcal{HG}_{2n,p,n}(t-x')}{\mathcal{HG}_{2n,p,n}(t-x)} \in \frac{\mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t-x')}{\mathcal{B}_{\frac{n}{2},\frac{p}{n}}(t-x)} \cdot (1 \pm \varphi_2(c) \cdot \frac{\log^{1.5}(n)}{\sqrt{n}}) \tag{61}$$

Applying Proposition A.7 with 'n' $= \frac{n}{2}$ and $\frac{p}{n}$, [**Iftach's Note: to do**] yields that

$$\frac{\mathcal{HG}_{2n,p,n}(t-x')}{\mathcal{HG}_{2n,p,n}(t-x)} \in \exp\left(\frac{-2(t-p)x + x^2 + 2(t-p)x' - x'^2}{n}\right) \cdot (1 \pm 2(\varphi_2(c) + \varphi_3(c))(\frac{\log^{1.5}(n)}{\sqrt{n}})),$$

where φ_3 is the function from Proposition A.7. We conclude the proof taking [**Iftach's Note: ..**] □